NICC ND 1631 V1.2.2 (2010-11)

NICC Document

NGN; PSTN/ISDN Service Interconnect; Architecture for usage of Common Numbering Database

Note : This standard was originally intended to allow fulfilment of changes to General Condition 18 which were announced by Ofcom via the November 2007 Statement entitled “Telephone number portability for consumers switching suppliers - Concluding Statement”. This change was subsequently set aside by the Competition Appeal Tribunal (Case 1094/3/3/08), and in the April 2010 Statement entitled “Routing calls to ported telephone numbers”, Ofcom concluded that no changes were justified.

However, Ofcom recognised the benefits that a common numbering database approach could bring both to number portability arrangements and to the conservation of geographic numbers, and further concluded that :

> *We consider that a direct routing solution for interconnected fixed networks using such an approach could become viable if and when next generation core network technology is adopted widely by network operators. While the timescale of such adoption is currently uncertain, we would encourage network operators to consider the benefits of incorporating direct routing capability into their next generation network designs.*

Accordingly, whilst NICC Standards cannot warrant what the precise model of usage of a common numbering database for future NGNs will be, this document provides an indication of what was considered appropriate when the issue was considered by NICC, and hence should be borne in mind by network operators when meeting Ofcom’s request to consider direct routeing when designing their NGNs.

Network Interoperability Consultative Committee,
Ofcom,
2a Southwark Bridge Road,
London,
SE1 9HA.

NOTICE OF COPYRIGHT AND LIABILITY

Copyright

Liability

If you have any comments concerning the accuracy of the contents of this document, please write to:

The Technical Secretary,
Network Interoperability Consultative Committee,
Ofcom,
2a Southwark Bridge Road,
London SE1 9HA.

Contents

Intellectual Property Rights

Pursuant to the NICC IPR Policy, no investigation, including IPR searches, has been carried out by NICC. No guarantee can be given as to the existence of other IPRs which are, or may be, or may become, essential to the present document.

Foreword

This NICC Document (ND) has been produced by NICC Naming Numbering and Addressing Working Group

Introduction

In November 2007 Ofcom published a Statement entitled “Telephone number portability for consumers switching suppliers” – “Concluding Statement”. In that statement Ofcom issued a Notification of modifications to General Condition 18. In that modification Communications Providers are required to establish a “Common Database” for the purposes of Number Portability. The present document sets out to fulfil the need to describe a technical solution for that “Common Database” irrespective of how and by whom it is used.

The present document has been produced by the NICC Naming Numbering and Addressing Working Group. It is an Architecture document, sometimes referred to as a Stage 2 document in the three stage standards development process. There are separate protocol specifications which elaborate the information flows contained in this architecture as implemented using particular protocols. The present document must be read in conjunction with those protocol specifications that are relevant to the chosen implementation in order to fully understand the requirements. The “Common Database” specified in the present document is intended to be used in conjunction with routeing capabilities in Softswitches and with Signalling Relay Functions. As a consequence of these dependencies this architecture cannot be properly understood in isolation.

Nothing in this document shall be taken as preventing the further elaboration of the specification contained herein for the purposes of specifying systems that are intended to be embodied in an implementation. Such further elaboration may be documented elsewhere and make reference to the present document.

1 Scope

The present document sets out the architecture to fulfil the requirement that networks be capable of routeing calls on an individual number basis to the correct terminating node.

2 References and Release Information

For the particular version of a document applicable to this release see ND1610 [10].

2.1 Normative references

The following referenced documents are indispensable for the application of this document.

[1] NICC, ND1633, UK Next Generation Networks; Element Naming Framework

[2] NICC, ND1617, Automated Business to Business (B2B) Transactions: Architecture and Principles

[3] NICC, ND1618, Profile for ebXML Messaging Service 2.0 Gateways

[4] Not used.

[5] IETF, RFC3261, SIP: Session Initiation Protocol

[6] IETF, RFC3966, The tel URI for Telephone Numbers

[7] IETF, STD 68, Augmented BNF for Syntax Specifications: ABNF

[8] NICC, ND1628, Signalling Security

[9] NICC, ND1208, Mobile Number Portability

[10] NICC, ND1610, Multi-Service Interconnect of UK Next Generation Networks

2.2 Release Information for Common Numbering Database

The NICC documentation to this version of the architecture for the use of the Common Numbering Database and applicable version of these documents is provided in [10].

3 Definitions, symbols and abbreviations

3.1 Definitions

For the purposes of the present document, the following terms and definitions apply:

Application Key : A key used only to sign transactions.

C-D Digit boundary : the boundary between the fifth and sixth digits in a UK telephone number including the leading zero.

NOTE: The standard format of a National Significant Number ('NSN') within the UK National Telephone Numbering Plan is notated as follows: 'SABCDEFGHI'. 'S' equates to the first digit after the '0' (for example S is 1 or 2 for Geographic Numbers). The C-D digit boundary is chosen as the dividing point for Sections of the Common Numbering Database so that all numbers with the same 0SABC prefix will be in the same Section e.g. for the number 01632 960123, C is '2' and D is '9': all numbers beginning 01632 will be in the same Section. Most geographic area codes comprise at least 3 digits after the S digit (i.e. ABC), hence this means that in many cases all numbers from a particular geographic area code will be contained in the same database Section.

Common Numbering Database : the generic function which holds reference mapping of telephone numbers to Destination Group. The Common Numbering Database is the general term for the set consisting of the Central Numbering Database and all copies of it held locally by individual CPs.

Central numbering database : The central reference database holding the mapping of telephone numbers to Destination Group.

Checkpoint Reference : an encoded data-time that represents a version of a Section of the Central numbering database. Each change to a Section (or set of changes that are taken together) results in a new checkpoint reference.

CP numbering database : A CP copy of the central numbering database.

Destination Group : A Destination Group represents a set of numbers (which may or may not be contiguous) served by a communications provider for which another provider would make the same routeing decisions for all numbers within it. Further information about Destination Groups can be found in Annex A of the present document.

Communications Provider (CP) : An entity providing communications services. For the purposes of this document, the delineation of which organisations qualify as Communications Providers is to be set by the telecoms regulator.

Date-time: A combination of date and time of an event. For the avoidance of doubt, all times shall be expressed in Greenwich Mean Time (GMT). In any period during which UK civil time is subject to a 1-hour positive offset, in accordance with the Summer Time Act 1972 (as amended), all times shall continue to be recorded in GMT.

Donor Communications Provider (Donor CP): In process terms, the Communications Provider which is currently the Owning Communications Provider for a number which is to be subject to Number Portability.

Key: A value used to create digital signatures.

Key Signing Key : A key used to sign other keys.

Number Group : A series of numbers (which need not be contiguous) which are grouped together for the purposes of being under the control of a single administrative entity. The numbers for which a CP is currently the Owning Communications Provider are partitioned into Number Groups which are not visible outside that CP.

Number Group Identifier: A CP-defined identifier for a Number Group.

Numbering Administrator : The agency responsible for the overall administration of the +44 UK numbering space. At the time of publication of the present document, this is Ofcom.

Owning Communications Provider (Owning CP): The Communications Provider which currently has rights to populate Administrative and Destination Group information associated with a number into the Common Numbering Database.

Pending Communications Provider (Pending CP): The Communications Provider which, following granting of permission by the Owning Communications Provider, has the right to take over control of the Administrative and Destination Group information associated with a number in the Common Numbering Database but has not yet done so.

Pre-Allocation Portability : A process to port numbers which have been allocated by Ofcom, but not yet assigned to end customers.

Recipient Communications Provider (Recipient CP): In process terms, the Communications Provider which will be the Owning Communications Provider for a number which is to be subject to Number Portability

Routeing function : takes the Destination Group from the Central/CP numbering database, and based on CP routeing policy, determines routeing of session/messages.

Section : A portion of the Central Numbering Database that can be downloaded independently of the remainder of it.

Service : For the purposes of this Green Release, this means IMS or PSTN (whether provided by TDM technologies or using a PSTN Emulation System)

3.2 Abbreviations

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

CDB	Central numbering DataBase
CP	Communications Provider
DG	Destination Group
DNS	Domain Name System
ebXML	Electronic Business using XML
IN	Intelligent Network
IRN	Intermediate Routeing Number, defined in [9]
MAP	Mobile Application Part (of C7 signalling)
SRF	Signalling Relay Function
XML	eXtensible Markup Language

4 Functional Entities and Interfaces

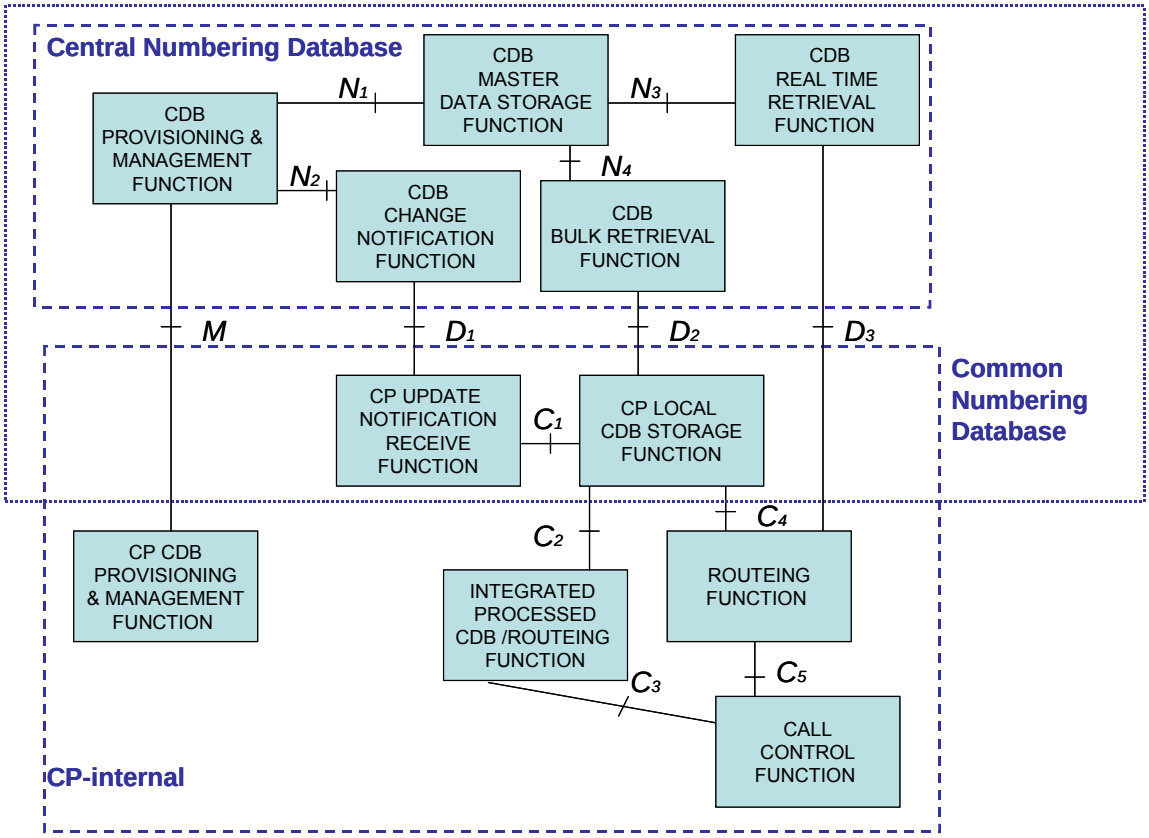

Figure 1 : Architecture

The functional architecture is depicted in Figure 1. Subject to the provisions of sub-clause 4.3.1.3 the Central Numbering Database **shall** support both the approach of real-time access and the approach of download of the database locally to CP networks ("Bulk Access"). The database **shall** be structured to allow CPs to choose to utilise both models according to number range.

Note : It is a CP matter whether the requirement to route directly is fulfilled;

- via implementation of a Routeing Function applying local policy in real time to the result of queries to the Central Numbering Database (hence reference points C_5 and D_3),
- via implementation of a Routeing Function applying local policy in real time to the result of queries of the local copy of the CDB (hence reference points C_1, C_4, C_5, D_1 and D_2),
- via implementation of a processed version of the CDB incorporating routeing information (hence reference points C_1, C_2, C_3, D_1 and D_2) or
- via a combination of these e.g. for different number ranges.

4.1 Functional Entities

4.1.1 CP Functions

4.1.1.1 Call Control Function

The role of the Call Control Function is to route the call in line with instructions received from the Routeing Function or Integrated Processed CDB/Routeing Function.

The Call Control Function **shall** query either the Routeing Function or Integrated Processed CDB/Routeing Function with the destination number, and if present Destination Group, to determine the route towards the Serving Call Control Function. It **shall** be possible to determine that the Common Numbering Database has been consulted by reference to the contents of the signalling passed between Call Control Functions; where no data was present for the destination number in the Common Numbering Database, then a default Destination Group **must** be populated in the called number information sent to subsequent Call Control Functions to indicate this, as specified in Annex C of the present document. Where the Common Numbering Database has yielded an answer, sufficient information **shall** be passed so that it is not necessary for networks to subsequently query the Common Numbering Database unless required for service interworking.

4.1.1.2 Routeing Function

The role of the Routeing Function is to take the destination information as provided by the Call Control Function and in conjunction with information from the Common Numbering Database together with local routeing policy instruct the Call Control Function how to process the call.

Where implemented, the Routeing Function **shall** accept requests from the Call Control Function, and respond with the preferred route(s) towards the Serving Control Function and sufficient information to populate signalling to subsequent Call Control Functions. This information **shall** include an indication that the call is being routed following interrogation of the Common Numbering Database. The Routeing Function **shall** process requests according to the logic set out in Annex C, which **may** result in a query to the Common Numbering Database. Local routeing policy **must** then be applied in real-time to the destination information received from the Call Control Function/Common Numbering Database (as appropriate).

Where the Call Control Function has provided insufficient information (e.g. number length too short), the Routeing Function **should** indicate the minimum number of digits required to fulfil the query. Where the Call Control Function has provided too many digits, unused digits **shall** be discarded.

4.1.1.3 Integrated Processed CDB/Routeing Function

The role of this Function is to take the destination information as provided by the Call Control Function and in conjunction with information from the Common Numbering Database and local routeing policy instruct the Call Control Function how to process the call. Unlike the standalone Routeing Function described previously, this is accomplished by pre-processing the local copy of the Common Numbering Database to incorporate the CP-specific routeing policy.

Where implemented, the Integrated Local CDB Copy/Routeing Function **shall** comprise the local copy of the Central Numbering Database, processed to incorporate CP-specific routeing policy. The manipulation **may** also include conversion of relevant Destination Groups to IRN form, where interworking with legacy technology is necessary and agreement with downstream networks for the use of IRNs has been reached.

The Integrated Local CDB Copy/Routeing Policy Function **shall** accept requests from the Call Control Function, and respond with the preferred route(s) towards the Serving Control Function and sufficient information to populate signalling to subsequent Call Control Functions. This information **shall** include an indication that the call is being routed following interrogation of the Common Numbering Database. The Routeing Function **shall** process requests according to the logic set out in Annex C of the present document, acting where necessary upon the integrated processed copy of the CDB.

Where the Call Control Function has provided insufficient information (e.g. number length too short), the Routeing Function **should** indicate the minimum number of digits required to fulfil the query. Where the Call Control Function has provided too many digits, unused digits **shall** be discarded.

4.1.1.4 CP Local CDB Storage Function

The role of this Function is to provide an up-to-date copy of part or all of the Common Numbering Database, held locally by the CP. This could be in order to remove any need for a CP-external real-time query to the Database, or could be in order to provide the ability to process the Database to incorporate local routeing policy.

The CP Local CDB Storage Function **shall** maintain a slave copy of the Central Numbering Database.

Where the CP Numbering Database is queried in real time:

1. The CP Numbering Database **shall** accept requests from the Routeing Function and within Timer T_{15} respond with the associated Destination Group information for the number.
2. Where the Routeing Function has provided insufficient information (e.g. number length too short), the CP Numbering Database **should** indicate the minimum number of digits required to fulfil the query. Where the Routeing Function has provided too many digits, unused digits **shall** be discarded.
3. A request associated with a number that has no Destination Group information populated (regardless of whether Administration Information has been populated to the database) shall result in an error response.

The CP Local CDB Storage Function **shall** download updates from the Central Numbering Database as instructed by the CP Update Notification Receive Function.

1. where the CP Local CDB Storage Function is queried in real-time it will be amended within Timer T_5 of a notified update from the CDB Change Notification Function to the CP Update Notification Receive Function.
2. where the CP Numbering Database is processed and the result incorporated into the Integrated Processed CDB/Routeing Function, this will be amended within Timer T_5 of a notified update from the CDB Change Notification Function to the CP Update Notification Receive Function.

NOTE 1: It is a CP matter how much of this specified time is dedicated to queuing notified updates to the database versus processing changes downloaded from the database.

NOTE 2 : See Clause 10 for Timer details

4.1.1.5 CP Update Notification Receive Function

The role of this Function is to monitor the Central Numbering Database for notifications of any changes to the Destination Group information, and where necessary to instruct the CDB Local Storage Function to download these changes.

The CP Update Notification Receive Function **shall** monitor for notifications from the Central Numbering Database that changes have been made to its contents. When notifications are received, it **shall** instruct the CP Local Database Storage Function to retrieve updates from the Central Numbering Database within a timeframe which allows the constraints in Section 4.1.1.4 to be achieved.

4.1.2 Central Numbering Database Functions

The Central Numbering Database **shall** support both real-time and bulk download models. It **shall** be possible for a CP to adopt one or the other model for each Section of the database. Performance of the real-time function **shall** not be impacted by the performance of the bulk download function (and vice versa), nor **shall** the performance experienced by one CP be impacted by the demands of another.

4.1.2.1 CDB Change Notification Function

The role of this Function is to notify those CPs that have subscribed to the relevant Sections of the Central Numbering Database when changes are made to the Destination Group information in the database, in order that up-to-date information can be downloaded.

The CDB Change Notification Function **shall** monitor for notifications from the CDB Provisioning and Management Function that changes have been made to the CDB Master Storage Function and distribute update notification messages to CP Update Notification Receive Functions.

4.1.2.2 CDB Bulk Retrieval Function

The role of this Function is to provide a download of changes that have been made to the Destination Group information in the Central Numbering Database since a given reference point and provide full copies of Sections.

The CDB Bulk Retrieval Function **shall** accept requests from the CP Local CDB Storage Functions and provide a response of all changes made to the relevant Section(s) of the CDB Master Storage Function since the time specified in the request.

4.1.2.3 CDB Real-Time Retrieval Function

The role of this Function is to provide responses to queries of the Destination Group information for a given number in real-time.

The CDB Real-Time Retrieval Function **shall** accept requests from the CP Routeing Function for the Destination Group information associated with a given telephone number and, within Timer T_{16}, provide the information.

4.1.2.4 CDB Master Storage Function

The role of this Function is to provide a reference database of the records associated with each telephone number.

For each valid number, the CDB Master Storage Function **shall** contain a series of records. These records shall be divided between those held for administrative purposes, and those relating to Destination Group information:

- Administrative information
  The administrative data includes a record of the CP with access privileges, together with the Number Group of which it is a member.

- Destination Group information

  The routeing data is a record of the associated Destination Group for a given service, and a time-to-live counter indicating the period for which the contents of the record may be locally cached. This time-to-live counter will be set at Timer T_4.

NOTE: See Clause 10 for Timer details

The CDB Master Storage Function shall process requests from the CDB Management and Provisioning function to query the status and change the contents of both the administrative and Destination Group information. It shall process requests from the CDB Bulk Retrieval Function to provide details of changes to Destination Group information since a specific time point. It shall process requests from the CDB Real-Time Retrieval Function to query the contents of Destination Group information for specified numbers.

The CDB Master Storage Function **shall** keep an archive of the state of the data records for a period equal to Timer T_{17}.

The Destination Group information held in the Central Numbering Database **shall** be partitioned into Sections and each Section **shall** be transferable independently. These Sections **must** be divisions of the number space. The database **shall** be partitioned at the C-D digit boundary.

NOTE: The intention of database partitioning is to allow a CP to keep local copies of the database entries for those Sections they believe are most relevant to them. For other numbers they could individually query the Central Numbering Database. Of course a CP **could** keep local copies of the whole database, or conversely **could** query the Central Numbering Database for all numbers.

4.1.2.5 CDB Management and Provisioning Function

The role of this Function is to provide a management interface to allow CPs (and relevant agencies) to change the data / associated access rights for information in the database.

The CDB Management and Provisioning Function **shall** provide a management interface to the Central Numbering Database to process the transactions set out in Clause 9 of the present document. The CDB Management and Provisioning Function **shall** hold records as set out in Clause 6 of the present document.

Access rights/restrictions **shall** be supported in line with regulatory requirements. The Central Numbering Database **must** support read access by all UK CPs, write access by the Owning CP and limited write access to the Pending CP for a given number.

4.2 Reference Points:

The Reference Points shown in Figure 1 have the following characteristics;

4.2.1 Reference Point D_1

Used to push notifications to CPs that the contents of the CDB have changed. CP and CDB external and specified in Clause 8 of the present document.

4.2.2 Reference Point D_2

Used by CPs to pull changes from the CDB. CP and CDB external and specified in Clause 8 of the present document.

4.2.3 Reference Point D_3

Used for real time access to Central Numbering Database to allow per session lookup. CP and CDB external and specified in Clause 8 of the present document.

4.2.4 Reference Point C_1

Used to carry instructions from the CP Update Receive Function to the CP Local CDB Storage Function to download updates. This Reference Point is an internal CP matter.

4.2.5 Reference Point C_2

Used to carry changes from the CP Local CDB Storage Function to update the CP Integrated Processed CDB/Routeing Function. This Reference Point is an internal CP matter.

4.2.6 Reference Point C_3

Used to carry real-time queries/responses between the Call Control Function and the CP Integrated Processed CDB/Routeing Function. This Reference Point is an internal CP matter.

4.2.7 Reference Point C_4

Used to carry real-time queries/responses between the Routeing Function and CP Local CDB Storage Function. This Reference Point is an internal CP matter.

4.2.8 Reference Point C_5

Used to carry real-time queries/responses between the Call Control Function and the Routeing Function. This Reference Point is an internal CP matter.

4.2.9 Reference Point M

Used to carry management information to populate the Central Numbering Database. CP and CDB external and specified in Clause 9 of the present document.

4.2.10 Reference Point N_1

Used to carry transactions and responses between the Central Database Provisioning and Management Function and the CDB Master Data Storage Function sufficient to fulfil the requirements of transactions on Reference Point M. This Reference Point is an internal Central Database Provider matter.

4.2.11 Reference Point N_2

Used to carry transactions and responses between the Central Database Provisioning and Management Function and the CDB Change Notification Function to highlight when the contents of the CDB Master Data Storage Function have changed. This Reference Point is an internal Central Database Provider matter.

4.2.12 Reference Point N_3

Used to carry transactions and responses between the CDB Real Time Retrieval Function and the CDB Master Data Storage Function sufficient to fulfil the requirements of transactions on Reference Point D_3. This Reference Point is an internal Central Database Provider matter.

4.2.13 Reference Point N_4

Used to carry transactions and responses between the CDB Bulk Retrieval Function and the CDB Master Data Storage Function sufficient to fulfil the requirements of transactions on Reference Point D_2. This Reference Point is an internal Central Database Provider matter.

4.3 Operational Modes

4.3.1 Read Access

4.3.1.1 Bulk Access

The Central Numbering Database **shall** provide a copy of its Destination Group information record contents to CPs on request.

The CP **shall** only be able to request a load of entire Sections, not partial Sections. The Central Numbering Database **shall not** filter the data, this is the prerogative of the CP.

The Central Numbering Database **shall** notify each subscribed CP Numbering Database using reference point D_1 within Timer T_3 in case of a notified update (e.g. number activation, number port). Requests for updates **shall** be fulfilled within Timer T_6.

NOTE: See Clause 10 for Timer details

Transfers over reference point D_2 **shall** include a digital error checking code so that a CP can have a high degree of confidence that they have a complete and correct transfer.

Each transfer over reference point D_2 **shall** include a checkpoint reference that uniquely identifies a checkpoint within the Central Numbering Database, for that Section. Each update of the Section by the Central Numbering Database **shall** generate a unique checkpoint reference. One update **may** include a batch of changes made to the Central Numbering Database.

The checkpoint reference **shall** be an algorithmic encoding of the date and time, to the nearest second, of when the Section was updated by the Central Numbering Database. The checkpoint reference **shall** continue to increment for at least 100 years from a defined start date, allowing for one increment per second for those 100 years.

4.3.1.2 Real-Time Access

The Central Numbering Database **shall** accept requests from the Routeing Function over reference point D_3 and respond within Timer T_{16} with the associated Destination Groups for the Services available via that number.

Where the Routeing Function has provided insufficient information (e.g. number length too short), the Central Numbering Database **shall** indicate the minimum number of digits required to fulfil the query. Where the Routeing Function has provided too many digits, extra digits **shall** be discarded.

A request associated with a number that has no Destination Group information populated (regardless of whether Administration Information has been populated to the database) shall result in an error response.

4.3.1.3 Splitting the read functionality of the Central Numbering Database

It could be decided that the Central Numbering Database should provide only bulk access; for example the provision of real-time access could be subject to competition between multiple providers. In this scenario, the Reference Point N_3 shall not be implemented. Bulk access to the data in the Central Numbering Database in order to subsequently provide a real-time interface would be via Reference Points D_1 and D_2. This is depicted in Figure 2.

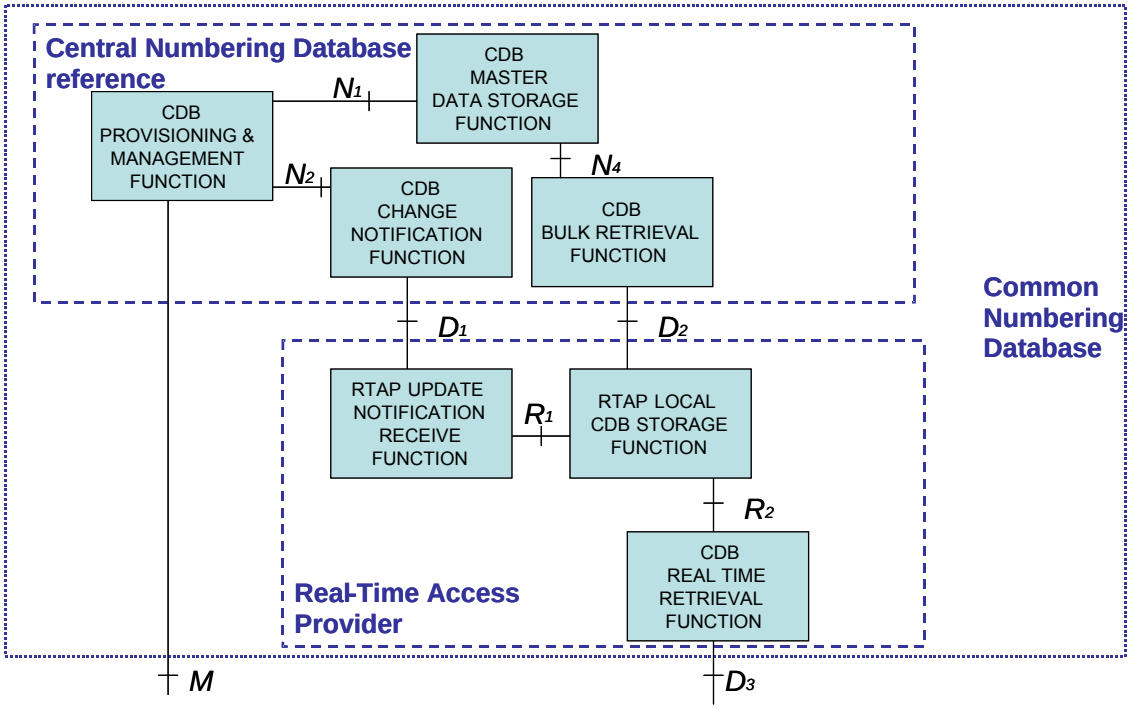

Figure 2:Splitting of read functionality of Central Numbering Database

The functions of the RTAP Local CDB Storage Function and the Real Time Access Provider Update Notification Receive Function shall be the same as those of the CP Local CDB Storage Function and the CP Update Notification Receive Function respectively.

4.3.2 Write Access

A management interface **shall** be provided to allow CPs to provision numbers into the Central Numbering Database. The interface **must** facilitate amendments to both individual and bulk numbers with appropriate security mechanisms so that only a CP authorised to make changes is able to do so. The transaction types set out in Clause 9 of the present document **shall** be supported.

4.4 Use Cases

The outline architecture described is functional and does not assume any implementation. Existing networks use standardised mechanisms such as IN and Mobile SRF's, the continued use of which should be permitted by the new architecture. In addition for NGNs there is a requirement that standardised architectures are designed with an expectation that ENUM will be used. This Sub-Clause sets out Use Cases for implementation of the functional architecture; it should not be considered exhaustive.

The following table sets out the protocol support requirements which result from the Use Cases set out in this Section.

Table 4.1: Reference Points and Protocol Use Cases

Reference Point	Protocol Support
M	Business to Business (B2B)
D_1	DNS $_{(notify)}$ or XML
D_2	DNS $_{(transfer)}$or XML
D_3	DNS $_{(ENUM)}$

Where multiple protocols are available CPs **may** opt to use different protocols for individual reference points.

4.4.1 Bulk Access using DNS to NGN

This is depicted in Figure 3. In this case the CP downloads a local copy of the reference database using DNS techniques. For the scenario depicted in Figure 3, the CP then processes this into a DNS-based server which incorporates data of both which terminating node a given number is hosted, and the routeing that this particular CP uses to direct calls towards that node.

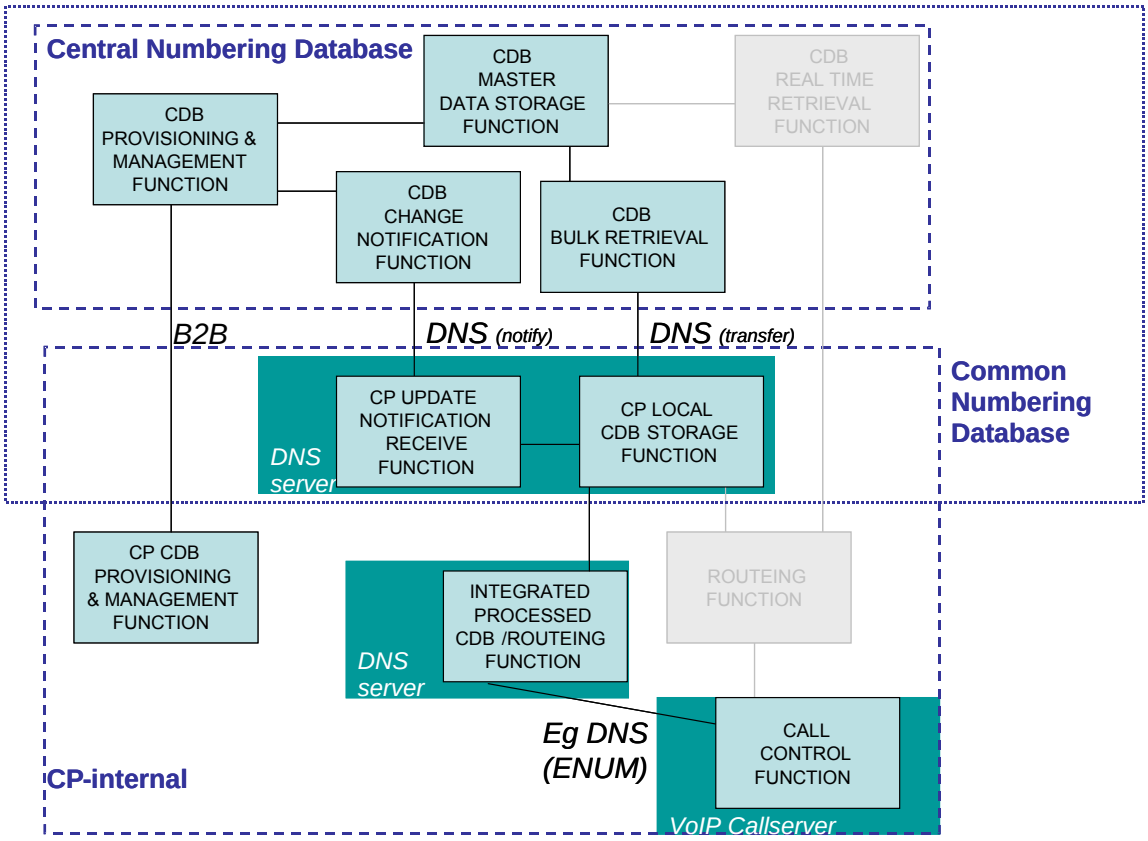

Figure 3 : Use Case for Bulk Access to database using DNS for NGN applications

4.4.2 Bulk Access using XML to NGN

This is depicted in Figure 4. In this case the CP downloads a local copy of the reference database using XML. As in the previous case, for the scenario depicted in Figure 4, the CP then processes this into a DNS-based server which incorporates data of both which terminating node a given number is hosted, and the routeing that this particular CP uses to direct calls towards that node.

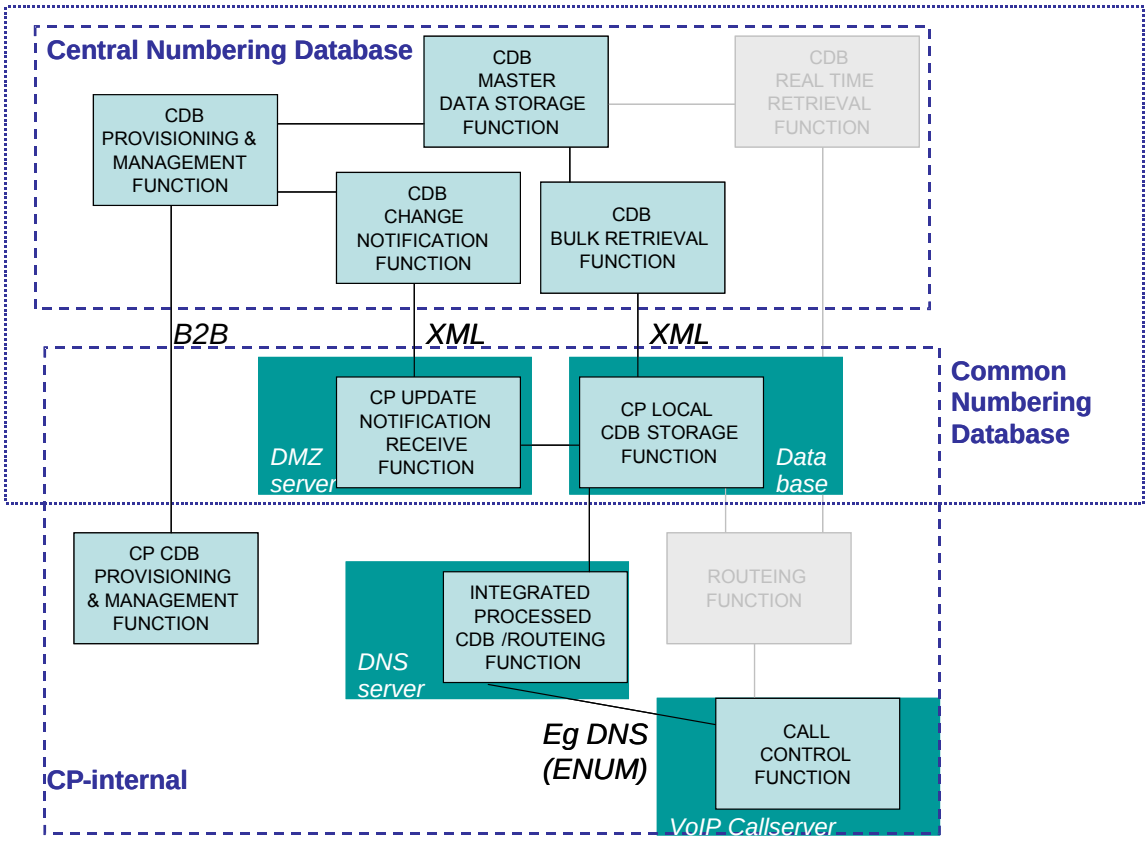

Figure 4 : Use Case for Bulk Access to database using XML for NGN applications

4.4.3 Bulk Access using XML to traditional mobile network

This is depicted in Figure 5. In this case the mobile CP downloads a local copy of the reference database using XML. Given they are specifically interested in Mobile Number Portability data and wish this to be in a form suitable for processing by traditional technology nodes, the relevant contents of the database are manipulated into the Intermediate Routeing Number (IRN) form set out in ND1208. This data is then used to populate the Signaling Relay Function (SRF) which is queried by the mobile switching nodes.

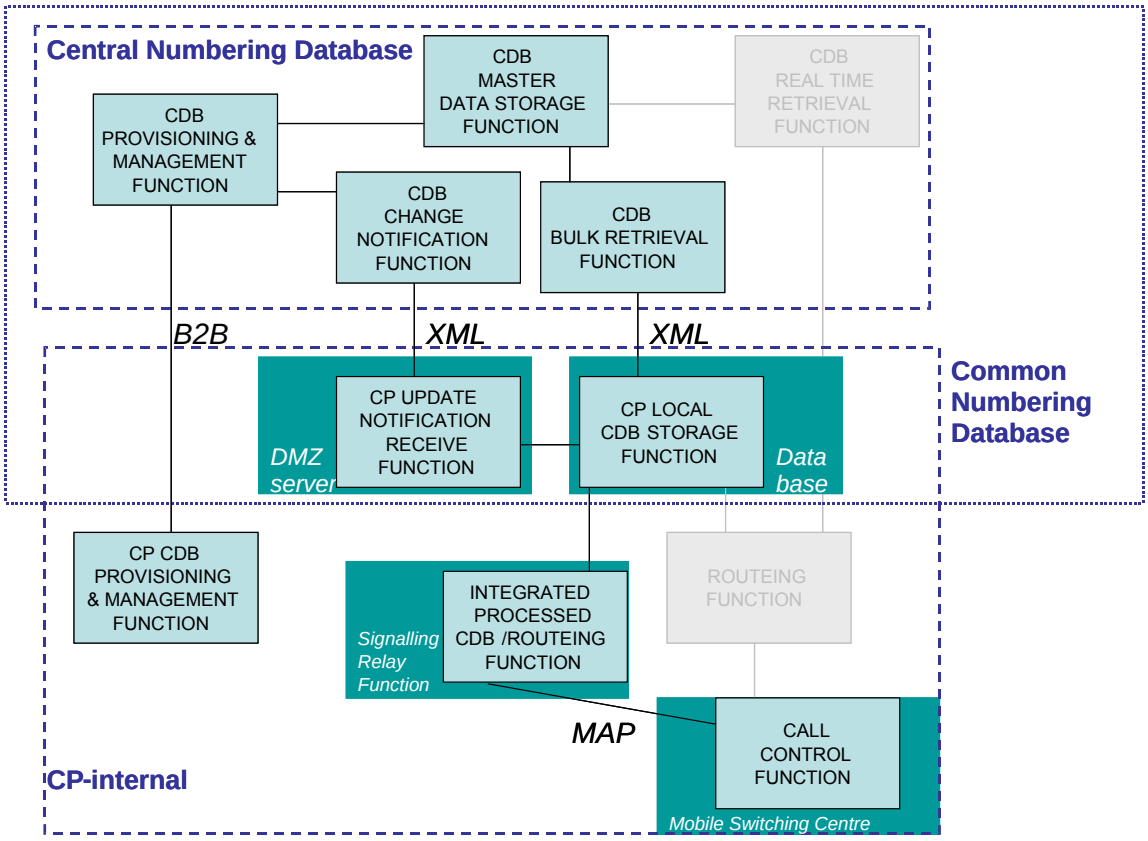

Figure 5 : Use Case for Bulk Access to database using XML for mobile applications

4.4.4 Real Time Access using DNS to NGN

This is depicted in Figure 6. In this case the CP queries the database in real-time using DNS.

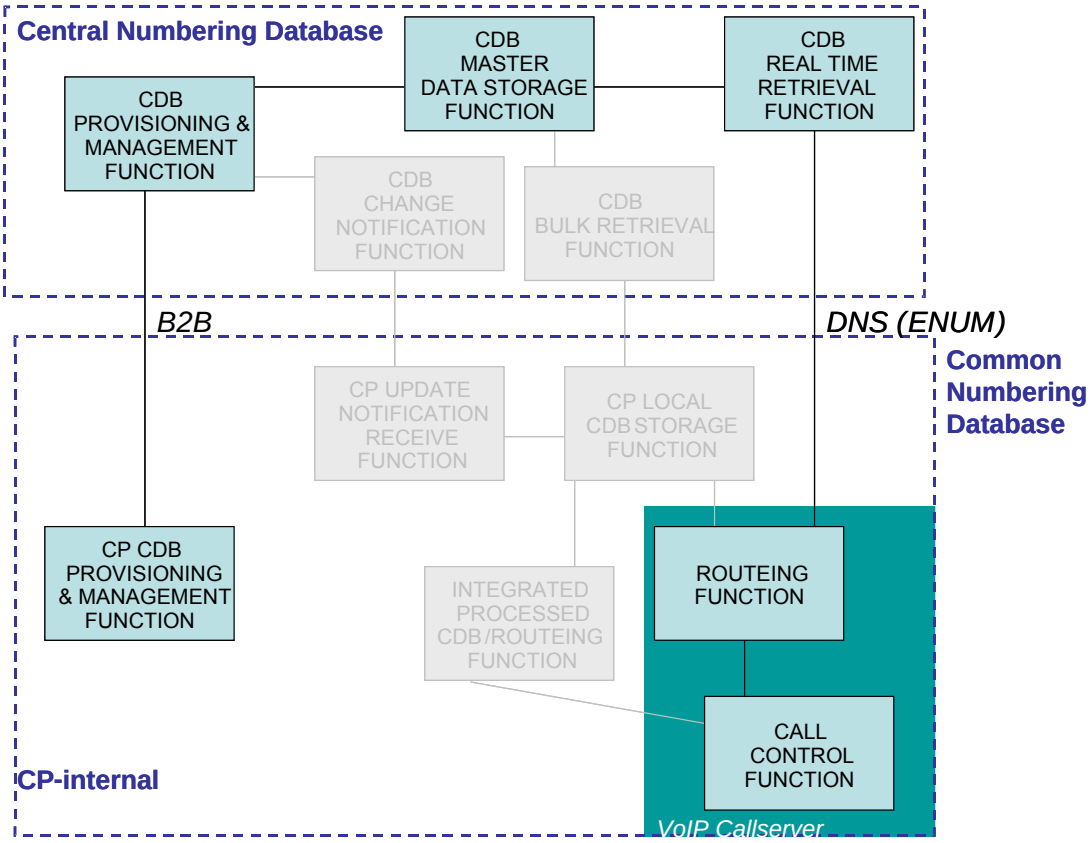

Figure 6 : Use Case for Real-Time Access to database using DNS

5 Security and Number Administration

This clause sets out the security policies to be used for all interfaces between the Central Numbering Database and CPs/Ofcom

5.1 Security Principles

Each operation **shall** be cryptographically signed, except where specified otherwise for performance reasons.

Each signed operation **shall** be individually signed, rather than rely on initial authentication and a subsequent secure channel.

Public key cryptography **shall** be used for all signatures, except where specified otherwise. This document makes no comment on what form of public key cryptography is used.

A signed document **shall** include an identifier for the sender and the signature shall be from a key known to be owned by that sender.

The systems **shall not** allow signatures to be repudiated either technically or because of the process used.

5.2 Interface security

Information Flows across the D_1, D_2 and D_3 reference points should be protected in accordance with the NICC requirement on Signalling Security, [8].

5.3 Number Groups

The Central Numbering Database **shall** allow a CP to partition the numbers they manage into different groups of numbers.

All CPs **shall** have one Default Number Group and **shall not** be required to create any more Number Groups unless they wish to.

The Central Numbering Database **shall** allow CPs to divide their numbers into groups as they wish with no restriction on the size of groups or the numbers they contain.

The Central Numbering Database **shall** allow CPs to assign a Number Group Identifier for use in later operations. These Identifiers are for use only between that CP and the Central Numbering Database and shall not be disclosed or otherwise used in transactions with other CPs.

5.4 Key Management

5.4.1 Types of keys

The Central Numbering database **shall** recognize two types of Key – Key-Signing Keys and Application Keys.

The two Key types have different purposes:

- Key-Signing Keys **shall** be used only for signing other keys and for operations relating to Key Management.
- Application Keys **shall** be used only to sign operations.

Certain Key-Signing Keys are designated as Root Key-Signing Keys; all other keys shall be signed (directly or indirectly) by a Root Key-Signing Key.

Each Application Key **shall** be signed by a Key-Signing Key. CPs may create a number of Intermediate Key-Signing Keys (Key-Signing Keys that are not Root Key-Signing Keys), thus creating a chain of Keys which **shall** ultimately be signed by a Root Key-Signing Key.

Note: use of Intermediate Key-Signing Keys serves two purposes:

1) It increases the security of the Root Key-Signing Keys.
2) It permits delegation of Key creation to different administrative functions or third parties

Keys may also have different scopes:

- CP-wide
- Number Group specific (see 5.4.4)

5.4.2 Key provisioning

Each CP and Ofcom **shall** register with the Central Numbering Database all the public keys they require the Central Numbering Database to use.

The Central Numbering Database **shall not** require or permit any CP or Ofcom to register private keys. CPs and Ofcom shall be responsible for keeping their own private keys private.

Each CP and Ofcom **shall** have at least one valid root Key-Signing Key registered with the Central Numbering Database at all times. Registration of the CP's initial Root-Key Signing Key is an out-of-band process completed as part of the CP setup.

When the CP registers or makes use of a key the Central Numbering Database **shall** check the key's validity by traversing the key's signature chain up to (and including) the CP's Root Key-Signing Key(s) and ensuring that there is at least one chain where every key in the chain is valid.

NOTE: In practice, this check only needs to be made when a key is registered and when another key in the chain expires or is revoked.

5.4.3 Key roll over

The Central Numbering Database **shall** allow each CP and Ofcom to have multiple public keys registered to allow effective roll over of the production keys they use. CPs **shall** specify the validity period of each of their keys at registration.

When any Key-Signing Key expires or is revoked , signatures created with it are no longer valid and therefore all other keys that were signed (directly or indirectly) by that Key shall have their validity re-evaluated as described in 5.4.2

To roll over an Intermediate Key-Signing Key a new key must be created and signed by the original parent Key or otherwise given a chain of signatures back to a Root Key-Signing Key. Then all existing Keys that were signed by the original Key should be re-signed using the new Key (though this is not necessary if there is an alternative chain to a Root not going through the original), and then those Keys in turn shall be re-registered with the Central Numbering Database.

5.4.4 Number Group Specific Keys

Application Keys and Intermediate Key-Signing Keys may be assigned to a specific Number Group. Root Key-Signing Keys shall not be assigned to a specific Number Group.

Keys cannot be assigned to more than one Number Group nor subsequently reassigned to another Number Group. A signature made using an Intermediate Key-Signing Key assigned to a specific Number Group is invalid if the signed key is not assigned to the same Number Group.

A CP **shall** assign at least one Application Key to each Number Group in use (including the Default Number Group). Management of that Number Group **shall** be restricted by the Central Numbering Database to CP-wide Keys and Keys that are associated with the Number Group. In some instances the Key is used to identify the Number Group to be used; in these instances, a CP-wide key **shall not** be used.

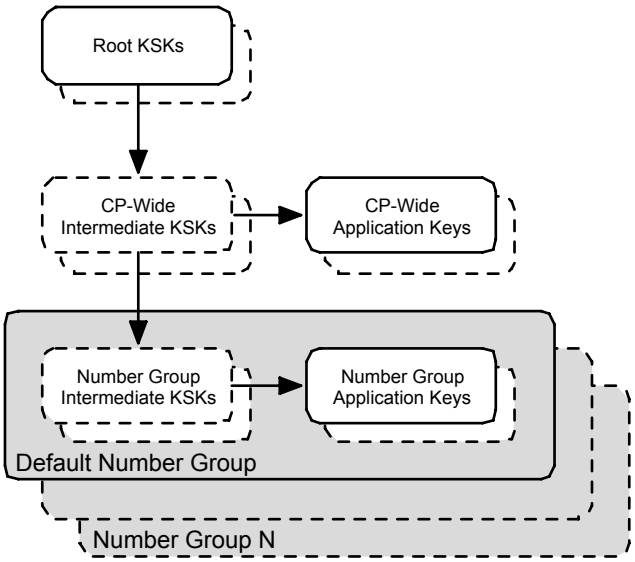

Figure 7 Types of Key used by CP

5.5.5 Override Function

There will be an override function for the Numbering Administrator and this will require a specific key (or keys) to be assigned to it. These keys must not be used for any other process. Currently this function is assigned to Ofcom.

The Numbering Administrator may use this function to issue any transaction (other than Upload, see Clause 9 of the present document) against any number, regardless of the Owning CP.

6 Central Numbering Database Contents

The Central Numbering Database **shall** contain the following information.

6.1 Number Section information

The CDB Master Storage Function **shall** hold a list of the Sections of the database, together with an indicator of whether each holds numbers.

6.2 CP information

The CDB Management Function **shall** hold the following information for each CP:

- The <*provider*> identity, in accordance with the UK NGN Network Element Naming Framework [1]
- List of PSTN Destination Group CP-identity values
- List of IMS Destination Group CP-label values
- List of CP Number Groups

The CDB Change Notification Function **shall** hold the following information for each CP;

- List of database Sections (if any) to which the CP has subscribed
- List of hosts which **shall** receive update notifications for all subscribed database Sections.

6.3 Key information

The CDB Management Function **shall** hold the following information for each CP Key:

- Public key data
- Owning CP
- Key type (root, intermediate or application)
- Valid or revoked
- Start date
- End date
- Number Group to which it applies, if any

6.4 Number information

For each valid number, the CDB Master Storage Function **shall** contain information, divided between that held for administrative purposes, and that relating to Destination Groups.

6.4.1 Administrative information

The CDB Master Storage Function **shall** hold the following information for each number:

- Owning CP
- Number Group
- Allocation certificate that was used to populate the database
- Pending CP (if applicable)
- Time at which Pending CP's permission to take ownership **shall** expire

The Administrative information **shall not** be made available via the D_2/D_3 interfaces.

6.4.2 Destination Group information

Where it has been populated, the CDB Master Storage Function **shall** hold Destination Group information, as specified in Annex A of the present document, for each number. The CDB Master Storage Function shall hold active Destination Group information.

Only active Destination Group information **shall** be made available via the D_2/D_3 interfaces.

6.4.3 Scheduled Requests

For each number the Central Numbering Database shall store a list of the outstanding Transaction IDs that affect the number and have not been cancelled.

6.5 Scheduled Requests Information

For each scheduled future change to Destination Group information, the following data shall be held:

- The CP making the change
- The transaction ID of the request
- The new Destination Group information
- The time window in which it will be made
- Whether this was a Data Upload or Take Change of Ownership
- The Application Key ID used to authorise the request
- The set of numbers affected by the change

7 Central Numbering Database usage

The present Clause provides examples of how the Central Numbering Database would be used in the lifecycle of a number. It is not intended to be exhaustive, but provides an insight into how the interfaces set out subsequently would be utilised. In the present clause transaction names are given in upper case, e.g. ALLOCATE, these names relate to information flows which are described in Clause 9 of the present document.

The figure below shows an example lifecycle for a number, in which a number is in use, ported twice and then disconnected and returned to the rangeholder.

In this example, the number has 4 possible states (Non-Normative):

- unallocated
- allocated
- routed (number contains routeing data)
- released (number is in the process of being ported)

Numbers in the “routed” and “released” state of this example would be downloaded to CPs using the D_2 or D_3 interface.

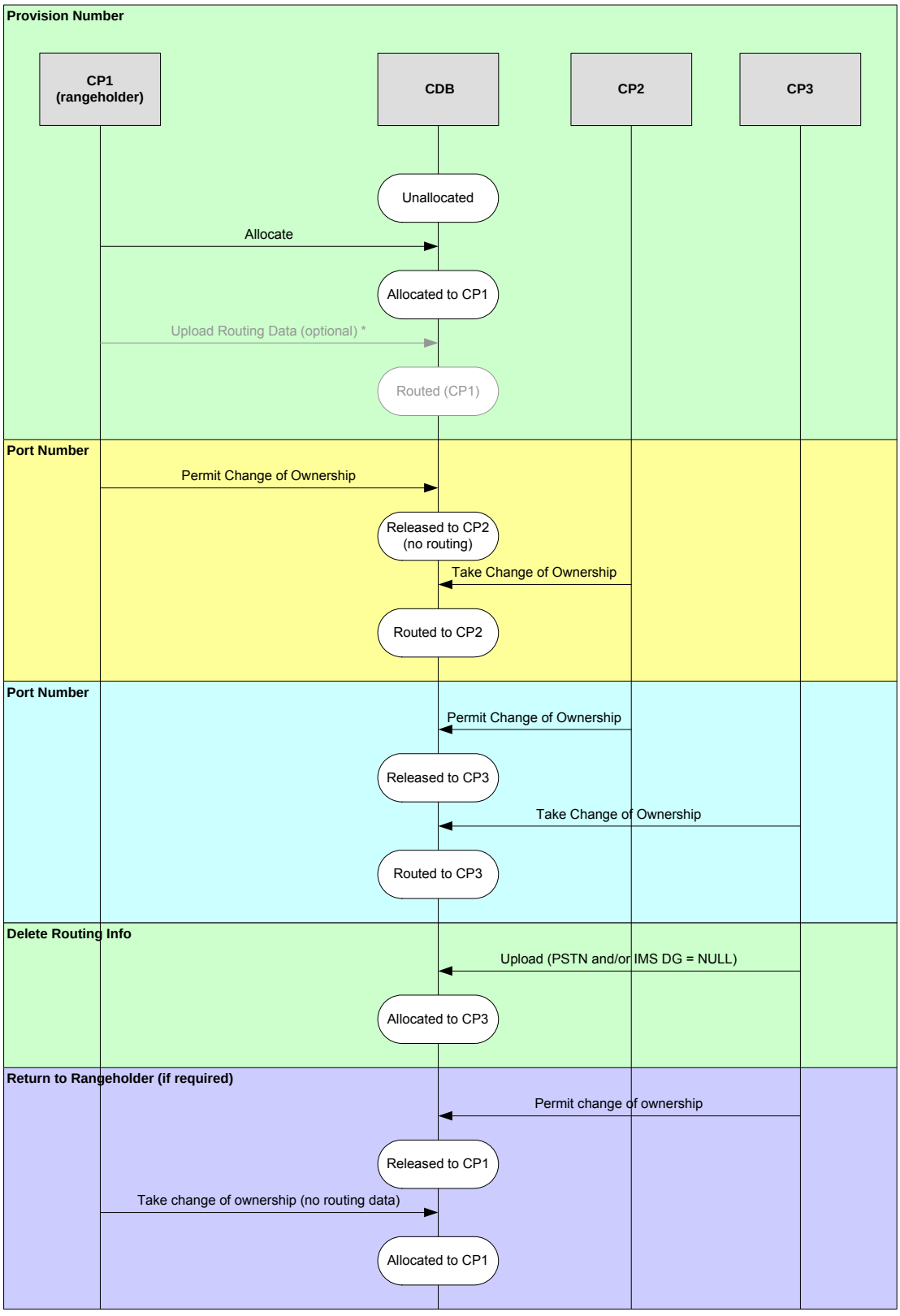

Figure 8 Example Life Cycle for a Number

7.1 Numbers are allocated by Ofcom

Numbers assigned by Ofcom will be accompanied by an allocation certificate. The CP will then use this to set the access rights for some or all of these numbers in the Central Numbering Database to one of their Number Groups using the ALLOCATE transaction. This Number Group will be under the control of a set of Application Keys, as described in Sub-clause 5.4. If the CP chooses to associate only a subset of the numbers allocated by Ofcom to the Number Group in question, then the Central Numbering Database will provide a residual certificate to the CP for it to subsequently use to associate the remaining numbers with Number Groups. Note that the original certificate can only be used once.

7.2 CP provisions numbers

A CP may choose whether to add routeing information to numbers in the database as part of the cycle of provisioning customers, or pre-provision to route traffic to a node in their network in advance of assigning the numbers to customers. Either way, the CP adds the routeing information using the UPLOAD transaction.

7.3 CP reconfigures their network

Where a CP chooses to reconfigure their network so that numbers are hosted on different nodes, hence different Destination Groups, the routeing information in the database is changed using the UPLOAD transaction.

7.4 Number is ceased

Where a CP ceases a number (e.g. because the customer no longer wishes to have service on that number), then the UPLOAD transaction may be used with both the Destination Group elements set to null. This removes the routeing information from the database, but leaves the access rights untouched.

7.5 Number is ported between networks

When a number is (or numbers are) to be ported, the donor CP will issue a PERMIT CHANGE OF OWNERSHIP transaction, which will unlock the records associated with the number to the recipient CP. The recipient CP will then issue a TAKE CHANGE OF OWNERSHIP transaction, which will change the Destination Group to which the number is routed. This TAKE CHANGE OF OWNERSHIP could be implemented immediately, or at a point in time dictated by the recipient.

It should be noted that a number need not have any Destination Group associated with it in order to enact the PERMIT CHANGE OF OWNERSHIP transaction, this could facilitate the Pre-Allocation Portability process.

7.6 Ported number is ceased

Where a number that has been ported is ceased, the architecture supports both a model in which the number is returned to the CP originally assigned it by Ofcom, or that the number is retained by the last CP that provided service on it.

For the model where the number is returned to the rangeholder CP, then a PERMIT CHANGE OF OWNERSHIP transaction is used by the CP that was providing service, followed by a TAKE CHANGE OF OWNERSHIP by the rangeholder, albeit with no associated routeing data records. This removes the routeing information from the database and returns the access rights to the range-holder CP.

NOTE: Determination of the rangeholder CP is beyond the scope of the present document.

For the model where the number is retained by the current CP, then the UPLOAD transaction is used with both the Destination Group elements set to null. This removes the routeing information from the database, but leaves the access rights untouched.

7. 7 Numbers are reclaimed by Ofcom

Where numbers are reclaimed by Ofcom, this is accomplished by a DELETE transaction being issued either by the CP or Ofcom (using Special Ofcom Privileges – this is one application of the over-ride key referred to in Clause 5.5.5 of the present document). This removes all data associated with the numbers from the database. A new allocation certificate will be required to bring the number back into use.

7.8 Usage of Number Groups

7.8.1 Number management is split across multiple departments within a CP

CPs that wish to split management of numbers across multiple departments can achieve this by having Number Groups under the control of specific Keys associated with each department.

7.8.2 Numbers are suballocated

CPs that wish to suballocate management of numbers, e.g. across. Multiple resellers, can achieve this by having Number Groups under the control of specific Keys associated with each reseller. It is a CP matter whether the reseller has direct control of the Number Group, or indirect control via a relevant department within the CP.

7.8.3 Number Group Management

The Number Group within which a given number is placed is initially determined by the Application Key which is used in the ALLOCATE transaction (i.e. the number will be placed within the Number Group to which the Application Key is associated). Similarly, where a number is ported from one CP to another, it is the Application Key which the recipient CP uses in the TAKE CHANGE OF OWNERSHIP transaction which determines which of their Number Groups the number will be imported into.

Should a CP wish to change the Number Group within which a number resides, this is treated as a number port, albeit with the same donor and recipient CP (i.e. the CP would issue a PERMIT CHANGE OF OWNERSHIP in favour of itself, then subsequently issue a TAKE CHANGE OF OWNERSHIP; the PCO transaction will use the Application Key associated with the Number Group from which the number should be moved, and the corresponding TCO transaction an Application Key associated with the Number Group to which the number should be moved).

7.9 Destination Group Management

CPs are allowed only to populate numbers in the CDB with their own Destination Group information. To police this, it is necessary for CPs to register the ranges of Destination Groups under their control with the CDB. It should be noted that the M interface does not make provision to add and remove Destination Group ranges from the CDB; this would be an offline activity.

7. 10 Hosting

It is possible to accommodate the commercial relationship whereby numbers are allocated to one CP by Ofcom, but then hosted by a third party CP network. In this situation the allocated CP would populate their Destination Groups in the database, but then arrange via network databuild for these Destination Groups to be routed to the host CP network.

7. 11 Disputes

From time to time, disputes may arise as to the ownership of a number. It is beyond the scope of the Central Numbering Database to resolve such disputes, but it can provide a valuable resource to those doing so.

The history of transactions for a given number can be ascertained using the HISTORY transaction. If this reveals that the status of the number is not in line with the expectation according to industry processes, then two options are available:

- If the CP which erroneously has access privileges is co-operative, then they can issue a PERMIT CHANGE OF OWNERSHIP transaction to the rightful owner, who would subsequently use a TAKE CHANGE OF OWNERSHIP transaction to assume ownership (defacto, the number is ported to the rightful assignee).
- If the CP which erroneously has access privileges is not co-operative, then via Ofcom involvement (see Sub-Clause 7.12) the ownership can be changed.

7.12 Special Ofcom Privileges

As the numbering plan administrator for the UK, Ofcom shall have special privileges over the operation of the database. In brief, this will allow:

1) Ofcom to forcibly change the access privileges for a number. This is accomplished via a TAKE CHANGE OF OWNERSHIP transaction, Ofcom's keys will have the ability to issue a Permit Change of Ownership transaction against any number in the CDB, after which the new owner can issue a TAKE CHANGE OF OWNERSHIP.

2) Ofcom to forcibly reclaim numbers. This is accomplished via a DELETE transaction.

3) Ofcom to audit usage of numbers. This is accomplished using an AUDIT transaction. The result will only indicate that numbers are to be routed but does not imply that an active end customer is using that number. As a consequence this mechanism cannot act as a substitute for the Ofcom Annual Numbering Audit.

7.13 Number Range Transfer

The transfer of a range of contiguous numbers needs no special operations within the database even if there are procedural differences in agreeing that this should happen. To accomplish the change, the procedures described in Sub-Clause 7.5 would be used.

8 Information Flows at the $D_1/D_2/D_3$ Reference Points

The Central Numbering Database **shall** allow a CP to host all or part of the database locally by taking copies of data in one of two ways; an incremental transfer of changes or a full load.

The incremental transfer process **shall** therefore be sufficiently robust that CPs can rely on this mechanism for data transfer without the need to initiate regular full loads for sanity checking.

Table 8.1: Summary of D_1, D_2 and D_3 Reference Points

Transaction	Summary of Usage
Notification (D_1)	A message sent by the CDB to a CP notifying them that a Section of the database has changed.
Full load (D_2)	Used by a CP to take a full copy of a Section of the CDB
Incremental (D_2)	Used by a CP to load the changes to a Section of the CDB.
Real Time (D_3)	Used by the CP to query the CDB for an individual number.

8.1 Notification (D_1) Information flow

8.1.1 Purpose

Used by the CDB to notify subscribed CPs of changes to Sections of the CDB.

8.1.2 Notification information elements

Table 8.2

M/O	Identity	*Notes*
M	ID	Transaction Identity
M	Section Notification	One or more Section notification items as defined below

8.1.2.1 Section Notification

Table 8.3

M/O	Identity	*Notes*
M	Section	The Section of the CDB that has changed
M	Checkpoint	The new checkpoint reference available for download.

8.1.3 Procedure

When a new set of changes for a subscribed Section is applied to the database, the Central Numbering Database **shall** create a new checkpoint and **shall** notify every CP subscribed to the changed Sections that a set of changes is now ready for download.

The Central Numbering Database **shall** send all notifications within Timer T_3 of their receipt of a change. In other words, from the time the Central Numbering Database receives a change, until the time when it has applied the change to the database and has notified all subscribed CPs that the change is available, **shall not** exceed Timer T_3 for any individual change.

NOTE: See Clause 10 for Timer details

The Central Numbering Database **shall not** send notifications any more frequently than Timer T_9 apart for the same database Section.

Where the specific protocol allows, the Central Numbering Database may include notifications for several Sections in one message. The semantics are the same as if separate notifications were used.

When a CP receives a notification it **may** then download that set of changes. Conversely the CP **may** choose to ignore some notifications if it so wishes, provided that it meets the overall service targets.

8.1.4 Response

Table 8.4

M/O	Identity	*Notes*
M	ID	Transaction Identity
M	Acknowledgement	Acknowledgement data that is specific to the particular protocol used.

8.2 Single Section Full download (D_2) Information flow

8.2.1 Purpose

The full load shall be used by a CP to retrieve the entire contents of a Section of the CDB.

8.2.2 Request information elements

Table 8.5

M/O	Identity	*Notes*
M	ID	Transaction Identity
M	Section	The Section of the CDB that a full download is requested for.

8.2.3 Procedure

The CDB shall return to the CP a copy of that Section of the database.. The CDB shall not filter the data in any way. The returned data shall include a checkpoint reference and an Error Checking Code.

The version of the Section sent in the response may be earlier than the current version. Therefore:

- after the download has been received, the CP **should** request an incremental download within Timer T_{14B} to ensure its version is then up-to-date.
- the version sent in the response **shall** be recent enough that during the period Timer T_{14B} a resulting incremental request will not be too old (see clause 8.3.3 of the present document);

8.2.4 Response information elements

Table 8.6

M/O	Identity	*Notes*
M	ID	Transaction Identity
M	Section	The Section of the CDB that a full download is of.
M	Checkpoint	The checkpoint reference for this set of data.
M	Data	The data of that Section of the database.
M	ECC	Error Checking Code

8.3 Single Section Incremental download (D_2) Information flow

8.3.1 Purpose

Used by a CP to request the changes to a Section of a CDB since a specified checkpoint reference and the current checkpoint reference.

8.3.2 Request information elements

Table 8.7

M/O	Identity	*Notes*
M	ID	Transaction Identity
M	Section	The Section of the CDB
M	Checkpoint	The checkpoint reference to use as the base for the incremental changes.

8.3.3 Procedure

When the CP requests a download of changes, it **shall** specify a Section and a checkpoint reference and the Central Numbering Database **shall** send all changes since that checkpoint, provided that the supplied checkpoint reference has not been obsoleted more than Timer T_{14A} in the past.

The Central Numbering Database **shall** keep up to Timer T_{14A} of changes in such a way as to allow a CP to request changes from any checkpoint in that period. If the supplied checkpoint reference is too old then the Central Numbering Database **may** refuse to send incremental changes, in which case the CDB **shall** send a bulk download response as if the request had been a bulk download request; the version downloaded **shall** be newer than the checkpoint reference in the request.

The set of changes **shall** include a checkpoint reference and an Error Checking Code.

The CDB **may** provide a second error checking code sufficient to allow the CP to confirm that its stored data for the relevant Section is undamaged. If so, the second ECC shall be accompanied by the checkpoint reference of the version of the data which it describes (the "ECC checkpoint") - this version **shall** be the same as would be returned in a request for a bulk download (see clause 8.2 of the present document). The CBD **shall** provide these values whenever the ECC checkpoint reference would be the same as either

- the checkpoint reference specified in the request or
- that specified in the response,

and **may** provide them with any other response.

Requesting an incremental download with the current checkpoint reference **shall not** generate an error – the Central Numbering Database **shall** return an empty update. Therefore a CP **shall** be able to safely request an incremental download without having been notified of a change.

8.3.4 Response information elements

Table 8.8

M/O	Identity	*Notes*
M	ID	Transaction Identity
M	Section	The Section of the CDB that this applies to.
M	Checkpoint	The current checkpoint reference for this set of data.
M	Data	The set of changes between the requested checkpoint reference and the current.
M	ECC	Error Checking Code
O	Full ECC	Error Checking Code data for the full Section
O	ECC Checkpoint	The checkpoint reference for the set of data used to compute the full ECC

8.4 Multiple Section download (D_2) Information flow

8.4.1 Purpose

Where the specific protocol allows, a CP may request downloads for more than one Section in a single request. It may request an arbitrary mixture of bulk and incremental downloads.

8.4.2 Request information elements

Table 8.9

M/O	Identity	*Notes*
M	ID	Transaction Identity
M	Requests	One or more individual requests, as specified in Table 8.10.

8.4.2.1 Requests

Table 8.10

M/O	Identity	*Notes*
M	Section	The Section of the CDB
M	Type	Full or Incremental
O	Checkpoint	The checkpoint reference to use as the base for the incremental changes; required for incremental requests, forbidden for bulk requests.

8.4.3 Procedure

The Central Numbering Database **shall** respond to each individual request either by returning data as specified in 8.2.3 or 8.3.3 as appropriate, or by returning an "omitted" response for that Section. It **shall** return data for at least one of the requested Sections.

8.4.4 Response information elements

Table 8.11

M/O	Identity	*Notes*
M	ID	Transaction Identity
M	Responses	One or more individual responses, one for each request. The individual responses **shall** either be as specified in clauses 8.2.4 or 8.3.4 of the present document, but omitting the ID element, or **shall** be the Omitted Response as specified in Table 8.12.

8.4.4.1 Omitted Response

Table 8.12

M/O	Identity	*Notes*
M	Section	The Section of the CDB that has changed
M	Type	Omitted

8.5 Real time query (D_3) information flow

8.5.1 Purpose

Used by a CP to query for the published routeing information for a specific number.

8.5.2 Request information flow

Table 8.13

M/O	Identity	*Notes*
M	Number	The number for which the Destination Group information is required

8.5.3 Procedure

The CP **shall** issue a query to Central Numbering Database for single number. The individual requests **shall not** include a cryptographic signature.

Each response **shall** be for a single number, not an aggregation of numbers. A response **shall** include a time to live that tells the CP how long the data is valid for. A CP **may** cache and reuse that information without issuing another request to the Central Numbering Database. A CP **shall not** continue to use that information for longer than the time to live.

The Central Numbering Database **shall** reply to every query within Timer T_{16}, excluding any network transfer time.

If the Common Database contains no Destination Group data for either PSTN or IMS then the response will take the form of an error result. The kind of error produced will be determined by the protocol used to implement the D_3 reference point. For the purposes of Annex C, when a CP receives an error of that type in response to a query of the database the "Nature of Result" shall be set to the value "neither type of URI present".

8.5.4 Response information flow

Table 8.14

M/O	Identity	*Notes*
M	Number	The number for which the routeing data is being returned
M	Routeing data	The Destination Group information for that number, or a record that indicates the number of digits required or that this is not a valid prefix.
M	Time to live	The time to live for that routeing data, Timer T_4

9 Information Flows at the M Reference point

The information flows at the M Reference point are intended to control the information specified in clause 6. For the purposes of the present Clause, references to "CP" shall include access by Ofcom using an Override Function.

Table 9.1

Transaction	Summary of Usage
Allocate	Used to reserve numbers as being under the control of a CP. The Central Numbering Database is amended to provide access rights of a specified set of numbers to the requesting CP. It is at the point where an Allocate transaction is issued against a given number that the administrative data records are populated.
Permit change of ownership	Used to allow a recipient CP to be given access rights to a number by a donor CP. On request of the CP with access rights to a specified set of numbers (the "Donor CP"), the Central Numbering Database shall be amended to provide access rights to a specified CP (the "Recipient CP").
Take Change of ownership	Used by a recipient CP to take access rights to a number from a donor CP and change the contents of records to route calls towards their network. On request of the Recipient CP that has been allowed access rights by the Donor CP, the Central Numbering Database will remove access rights of the Donor CP. This request will incorporate the record contents which the Recipient CP wishes to be implemented into the Common Numbering Database. It will be possible for the Recipient CP to specify that the transaction be implemented by the Common Numbering Database within Timer T_3 of a specified time, or within Timer T_3 of the request being submitted.
Upload	Used by a CP to change the contents of records on a non-urgent, urgent or timed basis. On request of the CP with appropriate access rights, the contents of the Common Numbering Database will be changed as stated for the specified numbers. The transaction has support for Critical, Not-Critical or Timed variants. It is at the point of activation of the first Upload transaction against a given number that communication data records will be populated
Cancel transactions	Used to cancel all active transactions against a telephone number
Delete number	Used to delete a number from the active database
Status and History query	Used to determine the changes in data associated with a particular number in a given period of time
Set Notified Servers	Indicates which servers a CP wishes to receive notifications about new Sections within the CDB
Subscribe	Used by a CP to subscribe to receive notifications of changes to a Section of the CDB
Unsubscribe	Used by a CP to unsubscribe from receiving notifications of changes to a Section of the CDB.
List subscriptions	Used by the CP to retrieve a list of the Sections of the CDB for which it is currently subscribed to receive changes.
Register Public key	Used by a CP to register security keys.
Revoke Public key	Used by a CP to revoke a security key.
Retrieve Public key	Used by a CP to list some or all of its keys registered with the CDB.
List Sections	Used by a CP to retrieve a list of all Sections of the CDB
Audit	Used by Ofcom to audit contents of database

9.1 Allocate Information Flow

This transaction shall be used by a CP to reserve a number or set of numbers as being controlled by them. It shall be used following initial assignment of numbers.

9.1.1 Purpose

This transaction shall be used by a CP to reserve a number or set of numbers as being controlled by them. It shall be used following initial assignment of numbers. At this stage, no Destination Group information is to be associated to the numbers.

9.1.2 Request Information Elements

Table 9.1.1

M/O	Identity	*Notes*
M	ID	Transaction Identity
M	Requesting Principal	Identity of CP sending request
M	Signing Key ID	Identity of the Application Key for the CP sending the request. This key must be assigned to a number group (which may be the default number group).
M	Signature	An electronic signature of the other information elements of this request, using the key identified by the Signing Key ID.
M	Numbers	A set of numbers (which need not be contiguous) which are to be added to the database.
M	Auth_Info	Either the allocation certificate as signed by Ofcom, or a residual allocation certificate as signed by the CDB.

9.1.3 Procedure

The CDB **shall** authenticate that the Application Key is valid for the CP and that the numbers have not already been assigned. The CDB **shall** authenticate that the set of numbers have been rightfully assigned by reference to either its own or the Ofcom public key as applicable. The CDB **shall** respond to an authorised transaction request with the information specified below. Where the request is valid, the numbers will be associated with the Number Group related to the Signing Key supplied. The certificate shall be invalidated to prevent later reuse.

.

9.1.4 Response Information Elements

Table 9.1.2

M/O	Identity	Notes
M	ID	Transaction Identity
M	Requesting Principal	Identity of CP sending request
M	Signing Key ID	Identity of the Key for the CDB
M	Signature	An electronic signature of the other information elements of this response, using the key identified by the Signing Key ID.
M	Response	The element **shall** take one of the following values: ACCEPT REJECT
M	Original Request	The data in the original request (so that the signature can assure non-repudiation by the CDB)
O	Reason	Where the Response element is set to ACCEPT this element **shall** be omitted. Where the Response element is set to REJECT, it **shall** take one of the following values; CP *(the App_key does not match the CP)* AUTH *(the authorisation information was not valid for some or all of the numbers)* ALREADY ASSIGNED *(all or some of the numbers have already been subject to an Allocate Information Flow)*
O	Residual	Where the Response element is set to REJECT this element **shall** be omitted. Where the Response element is set to ACCEPT; If the set of numbers in the request was identical to the set of numbers for which the Auth_Info applied then this element **shall** be omitted. If the set of numbers in the request was not identical to the set of numbers for which the Auth_Info applied then this element **shall** contain a digitally signed residual allocation certificate for the remaining numbers.

9.2 Permit change of ownership Information Flow

9.2.1 Purpose

This transaction **shall** be used by an Owning CP to indicate to the CDB that ownership of a number or set of numbers is to be changed (for example in the geographic number portability process, this transaction would be used by the Donor CP to indicate to the CDB that the number is approved to be ported and the record contents can be changed by the Recipient CP at their convenience).

9.2.2 Request Information Elements

The transaction request shall consist of the following parameters:

Table 9.2.1

M/O	Identity	Notes
M	ID	Transaction Identity
M	Requesting Principal	Identity of CP sending request
M	Signing Key ID	Identity of the Application Key for the CP sending the request.
M	Signature	An electronic signature of the other information elements of this request, using the key identified by the Signing Key ID.
M	Numbers	A set of numbers (which need not be contiguous) for which change of ownership is to be permitted.
M	Recipient_CP	Identity of CP that should be provided with access rights to the number(s) in question.
O	Transition	Where present, indicates that the transaction is being used as part of transitional arrangements.

9.2.3 Procedure

The CDB shall authenticate that the Application Key is valid for the CP issuing the request, for the number(s) in question and that there is not already a Pending CP recorded for the number(s) in question. The CDB shall be updated within Timer T_2 to cause the Recipient CP to be recorded as the Pending CP and therefore able to issue a Take Change of Ownership request against the number(s) in question. The CDB shall respond to the transaction request in the format as specified below.

Where the transaction is not followed by a successful Take Change of Ownership transaction (whether timed, urgent or non-urgent) within Timer T_7, the access rights for the number shall be returned to the original state, i.e there is no longer a Pending CP and nothing else is changed. It should be noted that the T_7 timer relates to when the Take Change of Ownership transaction is issued, not to when it is effected i.e. the ownership changes.

NOTE: See Clause 10 for Timer details

9.2.4 Response Information Element

Table 9.2.2

M/O	Identity	Notes
M	ID	Transaction Identity
M	Requesting Principal	Identity of CP sending request
M	Signing Key ID	Identity of the Key for the CDB
M	Signature	An electronic signature of the other information elements of this request, using the key identified by the Signing Key ID.
M	Response	The element **shall** take one of the following values: ACCEPT REJECT
M	Original Request	The data in the original request (so that the signature can assure non-repudiation by the CDB)
O	Reason	Where the Response element is set to ACCEPT this element **shall** be omitted. – Where the Response element is set to REJECT, it **shall** take one of the following values; CP *(the App_key does not match the CP)* AUTH *(the App_key is not authorised for the number(s))* PENDING CP (*the CP that should be provided access is unknown)* PENDING ALREADY *(A Pending CP already exists)*

9.3 Take Change of Ownership Information Flow

9.3.1 Purpose

This transaction **shall** be used by a Recipient CP to indicate to the CDB that ownership of a number or set of numbers is to be changed (for example in the geographic number portability process, this transaction would be used by the Recipient to indicate to the CDB that the number is to be transferred to the recipient and that in future access is to be denied to the Donor CP). It **shall** also be used by the Donor CP to revoke a Permit Change of Ownership transaction that was issued earlier and has not yet been acted upon.

NOTE 1: Agreement of the circumstances under which a Donor CP could revoke earlier permission is beyond the scope of the present document

NOTE 2: This transaction can only be issued following a Permit Change of Ownership.

9.3.2 Request Information Elements

The transaction request shall consist of the following parameters:

Table 9.3.1

M/O	Identity	Notes
M	ID	Transaction Identity
M	Requesting Principal	Identity of CP sending request
M	Signing Key ID	Identity of the Application Key for the CP sending the request. This key must be assigned to a number group (which may be the default number group).
M	Signature	An electronic signature of the other information elements of this request, using the key identified by the Signing Key ID.
M	Numbers	A set of numbers (which need not be contiguous) for which change of ownership is to be actioned and the record contents to be amended
M	Type	Not_Critical, Critical or Timed
O	Time	The GMT Date and Time required for change
M	PSTN_DG	Where a PSTN Destination Group is to be provisioned for the number(s), the identity of that PSTN Destination Group. Where no PSTN Destination Group is to be provisioned for the number(s), the value **shall** be set to null.
M	IMS_DG	Where an IMS Destination Group is to be provisioned for the number(s), the identity of that IMS Destination Group. Where no IMS Destination Group is to be provisioned for the number(s), the element value **shall** be set to null.
O	Transition	Where present, indicates that the transaction is being used as part of transitional arrangements.

9.3.3 Procedure

A Permit Change of Ownership shall always have been issued prior to a Take Change of Ownership.

The validation of the request shall be as follows:

1) The CDB shall perform the following checks for the number(s) in question and if either check fails returns a Reject response with reason AUTH:

   a. that there is a Pending CP, i.e. not empty/null, and

   b. that the Application Key is valid for the CP, i.e. it is either the Pending CP or the Owning CP.

2) If there is a scheduled Take Change of Ownership for the number(s) in question the CDB shall return a Reject response with reason PENDING.

3) The CDB shall verify that the PSTN and IMS Destination Groups (as applicable) are valid for the CP in question, otherwise providing a Reject response with reason PSTN_DG or IMS_DG as appropriate.

4) The CDB shall ensure that the scheduled time of the request, if present, is no further in the future than permitted by the process for the type of number involved.

If the transaction is valid, the CDB shall schedule a change to the Destination Group(s) and Administration information as follows:

- The contents of the CDB shall be changed within Timer T_8 for Non-Critical updates.
- For critical updates the update shall be completed as soon as capacity permits.
- For a timed request the CDB will check that capacity to propagate the request is anticipated to be available and reject the request (TIME_BUSY) if it is not available.

At the same time as the change is carried out, the Pending CP becomes the Owning CP (and thus the donor CP no longer has access rights), there is no longer a Pending CP and all timers associated with measurement of T_7 shall be reset. Any scheduled Data Upload requests by the Donor CP **shall** be deleted.

Where the request states that no Destination Group (i.e. either PSTN or IMS) is to be provisioned for the number(s), then no Destination Group data shall be provisioned for the number and any existing Destination Group data shall be removed.

It shall only be possible for one Take Change of Ownership transaction at a time to be scheduled for a given number.

NOTE: If a Take Change of Ownership is erroneously scheduled for the incorrect time, it is necessary to cancel that Take Change of Ownership and resubmit a correct Take Change of Ownership. It is not possible to over-write a Take Change of Ownership

9.3.4 Response Information Element

Table 9.3.2

M/O	Identity	Notes
M	ID	Transaction Identity
M	Requesting Principal	Identity of CP sending request
M	Signing Key ID	Identity of the Key for the CDB
M	Signature	An electronic signature of the other information elements of this response, using the key identified by the Signing Key ID.
M	Response	The element **shall** take one of the following values: ACCEPT REJECT
O	Reason	Where the Response element is set to ACCEPT this element **shall** be omitted. – Where the Response element is set to REJECT, it **shall** take one of the following values; CP *(the App_key does not match the CP)* AUTH *(the App_key is not authorised for the number(s)); either there has been no Permit Change of Ownership transaction issued for the number(s) in question, or it has not been in favour of the Requesting Principal)* PSTN_DG *(the PSTN Destination Group is not valid for the CP)* IMS_DG *(the IMS Destination Group is not valid for the CP)* INVALID_TIME *(The time requested is invalid)* TIME_BUSY *(There is no capacity to accept a transaction at the requested time)* PENDING (*A Take Change of Ownership transaction is already scheduled)*
M	Original Request	The data in the original request (so that the signature can assure non-repudiation by the CDB)

9.4 Upload Information Flow

9.4.1 Purpose

This transaction shall be used by the Owning CP to initially provision the Destination Group information associated with a number or set of numbers into the CDB. Additionally, it shall be used for changing the Destination Group information for a number or set of numbers in the CDB. In both cases, the timing of the changes may be not critical, critical or at a defined time.

9.4.2 Request Information Elements

The transaction request shall consist of the following parameters:

Table 9.4.1

M/O	Identity	Notes
M	ID	Transaction Identity
M	Requesting Principal	Identity of CP sending request
M	Signing Key ID	Identity of the Application Key for the CP sending the request.
M	Signature	An electronic signature of the other information elements of this request, using the key identified by the Signing Key ID.
M	Numbers	A set of numbers (which need not be contiguous) for which the record contents are to be amended
M	Type	Not_Critical, Critical or Timed
M	Skip_unauthorised	When set to true, numbers for which the Application Key is not valid **shall** be silently ignored. When set to false, if the Application Key is not valid for any Number the transaction **shall** fail.
O	Time	The GMT Date and Time required for change
O	PSTN_DG	Where a PSTN Destination Group is to be provisioned for the number(s), the identity of that PSTN Destination Group. Where no PSTN Destination Group is to be provisioned for the number(s), the value **shall** be set to null. Where this element is omitted, it shall indicate that the existing value of this element in the CDB should not be changed.
O	IMS_DG	Where an IMS Destination Group is to be provisioned for the number(s), the identity of that IMS Destination Group. Where no IMS Destination Group is to be provisioned for the number(s), the element value **shall** be set to null. Where this element is omitted, it shall indicate that the existing value of this element in the CDB should not be changed.
O	Existing_PSTN_DG	Where the change is to be applied only to that subset of Numbers which currently have a specific PSTN Destination Group, the value of that PSTN Destination Group. Where the change is to be applied only to that subset of Numbers with no PSTN Destination Group, the value **shall** be set to null. Where the change is to be applied irrespective of the existing PSTN Destination Group, then this element **shall** be omitted.
O	Existing_IMS_DG	Where the change is to be applied only to that subset of Numbers which currently have a specific IMS Destination Group, the value of that IMS Destination Group. Where the change is to be applied only to that subset of Numbers with no IMS Destination Group, the value **shall** be set to null. Where the change is to be applied irrespective of the existing IMS Destination Group, then this element **shall** be omitted.

9.4.3 Procedure

Where either Existing_PSTN_DG or Existing_IMS_DG are present, the CDB shall silently delete from the request those numbers which do not currently have the appropriate Destination Group(s). Then, the CDB shall authenticate that the Application Key is valid for the CP and for the number(s) in question. The CDB shall authenticate that the PSTN and IMS Destination Groups (as applicable) are valid for the CP in question. The CDB shall respond to the transaction request in the format as specified below. The contents of the CDB shall be changed within Timer T_8 for Non-Critical updates. For a timed request the CDB will check that capacity to propagate the request is anticipated to be available and reject the request if it is not available. The CDB shall ensure that the scheduled time of the request, if present, is no further in the future than permitted by the process for the type of number involved.

It shall be possible to have multiple Data Upload transactions scheduled for execution.

This transaction shall not affect whether there is a Pending CP for the number, any actions scheduled by that CP for the number, or the value of the T_7 timer associated with the Permit/Take Change of Ownership transactions.

NOTE: A CP could lose ownership of a number then regain it between the request being scheduled and executed. In this case the change *will not* take place, because the scheduled Upload will be removed as part of the execution of the first Take Change of Ownership.

9.4.4 Response Information Elements

Table 9.4.2

M/O	Identity	Notes
M	ID	Transaction Identity
M	Requesting Principal	Identity of CP sending request
M	Signing Key ID	Identity of the Key for the CDB
M	Signature	An electronic signature of the other information elements of this response, using the key identified by the Signing Key ID.
M	Response	The element **shall** take one of the following values: ACCEPT REJECT
O	Reason	Where the Response element is set to ACCEPT this element **shall** be omitted. – Where the Response element is set to REJECT, it **shall** take one of the following values; CP *(the App_key does not match the CP)* AUTH *(the App_key is not authorised for all of the number(s) and skip_unauthorised is false)* PSTN_DG *(the PSTN Destination Group is not valid for the CP)* IMS_DG *(the IMS Destination Group is not valid for the CP)* INVALID_TIME *(The time requested is invalid)* TIME_BUSY *(There is no capacity to accept a transaction at the requested time)*
M	Original Request	The data in the original request (so that the signature can assure non-repudiation by the CDB)

9.5 Cancel Transaction Information Flow

9.5.1 Purpose

This transaction shall be used to cancel pending transaction requests against a given set of numbers (for example in failure scenarios).

9.5.2 Request Information Elements

The transaction request shall consist of the following parameters:

Table 9.5.1

M/O	Identity	Notes
M	ID	Transaction Identity
M	Requesting Principal	Identity of CP sending request
M	Signing Key ID	Identity of the Application Key for the CP sending the request.
M	Signature	An electronic signature of the other information elements of this request, using the key identified by the Signing Key ID.
M	Cancel ID	Transaction to be cancelled

9.5.3 Procedure

The CDB shall authenticate that the Application Key is valid for the CP and for the Transaction in question. This includes the Application Key being valid for the Number Group of which the numbers (to which the Transaction related) is currently a member, or the Number Group of which the numbers were a member at the time of the request to be cancelled, or the key being any key from the default Number Group for the CP.

The following transactions may be cancelled, with the described effect (an attempt to cancel any other transaction **shall** fail):

Table 9.5.2

Transaction	Details	Effect
Take Change of Ownership	Cancellation is only permitted if the change, scheduled by the transaction being cancelled, is still scheduled and has not been carried out.	The effects of a successful cancellation is that the scheduled change is removed from the list of scheduled changes. The T7 timer is *not* reinstated.
Upload Information	Cancellation is only permitted if the change, scheduled by the transaction being cancelled, is still scheduled and has not been carried out.	The effects of a successful cancellation is that the scheduled change is removed from the list of scheduled changes

The CDB shall remove the pending request identified by the Transaction ID. The CDB shall respond to the transaction request in the format as specified below.

9.5.4 Response Information Elements

Table 9.5.3

M/O	Identity	Notes
M	ID	Transaction Identity
M	Requesting Principal	Identity of CP sending request
M	Signing Key ID	Identity of the Key for the CDB
M	Signature	An electronic signature of the other information elements of this response, using the key identified by the Signing Key ID.
M	Response	The element **shall** take one of the following values: ACCEPT REJECT
O	Reason	Where the Response element is set to ACCEPT this element **shall** be omitted. – Where the Response element is set to REJECT, it **shall** take one of the following values; CP *(the App_key does not match the CP)* AUTH *(the App_key is not authorised for the number(s))* CANT *(The transaction is incapable of being cancelled)*
M	Original Request	The data in the original request (so that the signature can assure non-repudiation by the CDB)

9.6 Delete Number Information Flow

9.6.1 Purpose

This transaction **shall** be used to remove a number or set of numbers from the database outright.

9.6.2 Request Information Elements

The transaction request shall consist of the following parameters:

Table 9.6.1

M/O	Identity	Notes
M	ID	Transaction Identity
M	Requesting Principal	Identity of CP sending request
M	Signing Key ID	Identity of the Application Key for the CP sending the request.
M	Signature	An electronic signature of the other information elements of this request, using the key identified by the Signing Key ID.
M	Numbers	A set of numbers (which need not be contiguous) for which the deletion is to be applied

9.6.3 Procedure

The CDB shall authenticate that the Application Key is valid for the CP and for the number(s) in question. The number(s) and all associated data (except historical records) shall be removed from the database. The CDB shall respond to the transaction request in the format as specified below.

9.6.4 Response Information Elements

Table 9.6.2

M/O	Identity	Notes
M	ID	Transaction Identity
M	Requesting Principal	Identity of CP sending request
M	Signing Key ID	Identity of the Key for the CDB
M	Signature	An electronic signature of the other information elements of this response, using the key identified by the Signing Key ID.
M	Response	The element **shall** take one of the following values: ACCEPT REJECT
O	Reason	Where the Response element is set to ACCEPT this element **shall** be omitted. – Where the Response element is set to REJECT, it **shall** take one of the following values; CP *(the App_key does not match the CP)* AUTH *(the App_key is not authorised for the number(s))*
M	Original Request	The data in the original request (so that the signature can assure non-repudiation by the CDB)

9.7 Status and History Query Information Flow

9.7.1 Purpose

This transaction **shall** be used to determine the history of a given number. This transaction **shall also** be used to verify which CP has (CPs have) administrative rights for a given number.

9.7.2 Request Information Elements

The transaction request shall consist of the following parameters:

Table 9.7.1

M/O	Identity	Notes
M	ID	Transaction Identity
M	Requesting Principal	Identity of CP sending request
M	Signing Key ID	Identity of the Application Key for the CP sending the request.
M	Signature	An electronic signature of the other information elements of this request, using the key identified by the Signing Key ID.
M	Number	A number for which history is being queried
O	Start Date	The date-time from which the history is required.
O	End Date	The date-time to which the history is required. If not present, then a default date-time of present time is used.
NOTE: If both optional elements are omitted only the current status is requested		

9.7.3 Procedure

The CDB **shall** authenticate that the Application Key is valid for the CP. The CDB **shall** respond to the transaction request in the format as specified below. The information **shall** be obtained from historic data held in the CDB Management and Provisioning Function. The CDB **shall** keep data for the period of Timer T_{17}.

9.7.4 Response Information Elements

Table 9.7.2

M/O	Identity	Notes
M	ID	Transaction Identity
M	Requesting Principal	Identity of CP sending request
M	Signing Key ID	Identity of the Key for the CDB
M	Signature	An electronic signature of the other information elements of this response, using the key identified by the Signing Key ID.
M	Response	The element **shall** take one of the following values: ACCEPT REJECT
O	Reason	Where the Response element is set to ACCEPT this element shall be set be omitted. Where the Response element is set to REJECT it shall take one on the following values: CP *(the App_key does not match the CP)* AUTH *(the App_key is not authorised for the number(s))*
O	Historic Data	Where the Response element is set to ACCEPT, a sequence of at least one Historic Data Elements as defined below
O	Timeout	If applicable, the element **shall** identify the date on which the Pending CP's right to issue a Take Change of Ownership Request will be revoked..

9.7.4.1 Historic Data Element

The data elements in the following table are appropriate to a period of time which starts at the identified Time/Date and remains valid unless changed by a subsequent set of data elements. The response to a History Query will always contain at least one set of Historic Data but may contain more than one.

Table 9.7.3

M/O	Identity	Notes
M	Time/Date	The date from which the current set of data applied
M	Transaction ID	Transaction Identity that gave effect to this change
C	Owning CP	The identity of the CP which had access rights from Time-Date, If this value is not present it indicates that the number was deleted from the CDB
C See Note	Pending CP	The identity of the CP that is permitted to issue a Take Change of Ownership request as at Time/Date
C See Note	PSTN Content	PSTN records which were applied at Time-Date
C See Note	IMS Content	The IMS records which were applied at Time-Date
O	Group	If the Owning CP is also the Requesting Principal, the Number Group Identifier that applied at Time/Date
NOTE: M/O value C represents Conditional Mandatory – the element is Mandatory if it was present at the Time/Date but omitted if it was not present at that Time/Date		

9.8 Set Notified Servers Information Flow

9.8.1 Purpose

This transaction shall be used by a CP to indicate the servers to which every notification of changes to subscribed Sections of the CDB shall be sent.

9.8.2 Request information Elements

Table 9.8.1

M/O	Identity	Notes
M	ID	Transaction Identity
M	Requesting Principal	Identity of CP sending request
M	Signing Key ID	Identity of the Application Key for the CP sending the request. This must be a CP-wide key.
M	Signature	An electronic signature of the other information elements of this request, using the key identified by the Signing Key ID.
M	Recipients	A list of host names or IP addresses, to a maximum of five, of the servers that are to receive all of the notifications.
M	Protocol	For each of the Recipients, which protocol is to be used to send notifications to that Recipient.

9.8.3 Procedure

Server host names must be appropriate, e.g. not localhost or 127/8. The determination of what addresses are appropriate is implementation dependent.

When the supplied server addresses have been verified as reachable and appropriate their verified values, and only those values, shall be used for all future notifications. The list of notified servers is not cumulative and any servers notified on previous request but not included in the latest request will not receive notifications after the transaction is actioned.

In order to allow clarity, if any server is not accepted the whole transaction is rejected, the request shall not be partially implemented.

The transaction shall be either accepted and actioned or rejected within Timer T_{11} of receiving the request.

NOTE: each server has an associated protocol to be used to notify it; different protocols may be used for different servers.

9.8.4 Response Information Elements

Table 9.8.2

M/O	Identity	Notes
M	ID	Transaction Identity
M	Requesting Principal	Identity of CP sending request
M	Signing Key ID	Identity of the Key for the CDB
M	Signature	An electronic signature of the other information elements of this response, using the key identified by the Signing Key ID.
M	Response	The element **shall** take one of the following values: ACCEPT REJECT
O	Reason	Where the Response element is set to ACCEPT this element shall be set be omitted. Where the Response element is set to REJECT it shall take one on the following values: CP *(the App_key does not match the CP)* AUTH *(the App_key is not authorised for the number(s))* INVALID HOST INVALID IP ADDRESS INVALID PROTOCOL
M	Original Request	The data in the original request (so that the signature can assure non-repudiation by the CDB)

9.9 Subscribe Information Flow

9.9.1 Purpose

This transaction shall be used by a CP to subscribe to notifications of changes to a Section of the CDB

9.9.2 Request information Elements

Table 9.9.1

M/O	Identity	Notes
M	ID	Transaction Identity
M	Requesting Principal	Identity of CP sending request
M	Signing Key ID	Identity of the Application Key for the CP sending the request. This must be a CP-wide key.
M	Signature	An electronic signature of the other information elements of this request, using the key identified by the Signing Key ID.
M	Sections	A set of Sections (which need not be contiguous) for which the subscribe is requested. Each Section is sent as a partial number with the last digit being the C digit.

9.9.3 Procedure

If the CP is not yet subscribed to any of the Sections requested, the CDB **shall** add the new subscriptions and **shall** start sending notifications within Timer T_{10} of receiving the subscribe request. The CDB **shall** authenticate that the Application Key is valid for the CP.

In all cases the CDB shall respond with the information below.

9.9.4 Response information Elements

Table 9.9.2

M/O	Identity	Notes
M	ID	Transaction Identity
M	Requesting Principal	Identity of CP sending request
M	Signing Key ID	Identity of the Key for the CDB
M	Signature	An electronic signature of the other information elements of this response, using the key identified by the Signing Key ID.
M	Response	The element **shall** take one of the following values: ACCEPT REJECT
O	Reason	Where the Response element is set to ACCEPT this element **shall** be omitted. – Where the Response element is set to REJECT, it **shall** take one of the following values; AUTH (The Requesting Principal does not have authority to make this request) SECTION (The Section specified is not valid)
M	Original Request	The data in the original request (so that the signature can assure non-repudiation by the CDB)

9.10 Unsubscribe Information Flow

9.10.1 Purpose

This transaction shall be used by a CP to unsubscribe to notifications of changes to a Section of the CDB that it is already subscribed to.

9.10.2 Request information Elements

Table 9.10.1

M/O	Identity	Notes
M	ID	Transaction Identity
M	Requesting Principal	Identity of CP sending request
M	Signing Key ID	Identity of the Application Key for the CP sending the request. This must be a CP-wide key.
M	Signature	An electronic signature of the other information elements of this request, using the key identified by the Signing Key ID.
M	Section	The Section of the database to be the subject of the unsubscribe operation. This is sent as a partial number with the last digit being the C digit.

9.10.3 Procedure

The CDB shall cease sending notifications within Timer T_{12} of receiving the unsubscribe request. If the CP does not have an existing subscription then the CDB shall respond to that effect but make no change to the database. In all cases the CDB shall respond with the information below. The CDB **shall** authenticate that the Application Key is valid for the CP.

9.10.4 Response information Elements

Table 9.10.2

M/O	Identity	Notes
M	ID	Transaction Identity
M	Requesting Principal	Identity of CP sending request
M	Signing Key ID	Identity of the Key for the CDB
M	Signature	An electronic signature of the other information elements of this response, using the key identified by the Signing Key ID.
M	Response	This element **shall** take one of the following values: ACCEPT REJECT
O	Reason	Where the response element is set to ACCEPT this element shall be omitted. Where the Response element is set to REJECT it shall take one of the following values: AUTH (The Requesting Principal does not have authority to make this request) SECTION (The Section specified is not valid) NOT_SUBSCRIBED (The Requesting Principal is not subscribed to the specified Section)
M	Original Request	The data in the original request (so that the signature can assure non-repudiation by the CDB)

9.11 List subscriptions Information Flow

9.11.1 Purpose

This transaction shall be used by a CP to request a list of the Sections to which they are currently subscribed, and will therefore receive notifications of changes to the contents of those Sections.

9.11.2 Request information Elements

Table 9.11.1

M/O	Identity	Notes
M	ID	Transaction Identity
M	Requesting Principal	Identity of CP sending request
M	Signing Key ID	Identity of the Application Key for the CP sending the request. This must be a CP-wide key.
M	Signature	An electronic signature of the other information elements of this request, using the key identified by the Signing Key ID.

9.11.3 Procedure

The CDB shall respond with a full list of the subscriptions and the recipient data within Timer T_{13} of receiving the request. The CDB **shall** authenticate that the Application Key is valid for the CP.

9.11.4 Response information Elements

Table 9.11.2

M/O	Identity	Notes
M	ID	Transaction Identity
M	Requesting Principal	Identity of CP sending request
M	Signing Key ID	Identity of the Key for the CDB
M	Signature	An electronic signature of the other information elements of this response, using the key identified by the Signing Key ID.
M	Response	The element **shall** take one of the following values: ACCEPT REJECT
O	Reason	Where the Response element is set to ACCEPT this element shall be set be omitted. Where the Response element is set to REJECT it shall take one on the following values: CP *(the App_key does not match the CP)* AUTH *(the App_key is not authorised for the number(s))*
C See Note	Server_List	The list of servers to which the notifications are sent.
C See Note	Protocol_List	The list of protocols used, corresponding to the notified servers
C See Note	Sections	A sequence of at least one Section of Database as defined below
NOTE: M/O value C is Mandatory if Response element is set to ACCEPT and optional otherwise		

9.11.4.1 Section of Database

Table 9.11.3

M/O	Identity	Notes
M	Section	A Section of the database to which the requesting CP is subscribed. This is sent as a partial number with the last digit being the C digit.

9.12 Register Public Key Information Flow

9.12.1 Purpose

Used by a CP to register the public keys they will be expecting the CDB to recognise and to re-register a key with additional signatures.

9.12.2 Request information elements

Table 9.12.1

M/O	Identity	Notes
M	ID	Transaction Identity
M	Requesting Principal	Identity of CP sending request
M	Signing Key ID	Identity of the Application Key for the CP sending the request or, if the CP has no appropriate Application keys registered, the identity of a Root Key-Signing key.
M	Signature	An electronic signature of the other information elements of this request, using the key identified by the Signing Key ID.
M	Key ID	The ID of the key derived from the key using the standard ID mechanism for that type of key.
M	KeyData	The public portion of the key
M	Type	Specifies the type of key that this is ROOT INTERMEDIATE APPLICATION
M	StartDate	The date and time (GMT) from which this key will become valid
M	EndDate	The date and time (GMT) at which this key will expire
O	Group	If this Key applies to a non-default Number Group then its identifier should be specified here. If the Key applies to the default Number Group, then this should be nil. If the Key is CP-wide, or is one that has previously been registered, then this should be omitted.

9.12.3 Procedure

The CDB shall authenticate that the Key signing the transaction is valid for the CP. If the Key is not to be associated with a Number Group, the CDB shall verify that the signing key is a CP-wide one.

Where the Key is a new one, the CDB shall authenticate all the signatures on the key. Where the Key is an existing one, the CDB shall authenticate any new signatures. In each case, all the signatures that are authenticated (but not any previously existing ones) shall be required to be valid. The CDB shall also validate the Key Signature chain.

The Central Numbering Database **shall not** require any CP or Ofcom to register private keys. CPs and Ofcom **shall** be responsible for keeping all private keys private.

A CP/Ofcom **shall** have at least one valid root Key-Signing Key registered with the Central Numbering Database at all times.

The CDB **shall not** accept any keys that have been previously revoked.

9.12.4 Response information elements

Table 9.12.2

M/O	Identity	Notes
M	ID	Transaction Identity
M	Requesting Principal	Identity of CP sending request
M	Signing Key ID	Identity of the Key for the CDB
M	Signature	An electronic signature of the other information elements of this response, using the key identified by the Signing Key ID.
M	Key ID	The ID of the key derived from the key using the standard ID mechanism for that type of key.
M	Response	The element **shall** take one of the following values: ACCEPT REJECT
O	Reason	Where the response element is set to ACCEPT this element shall be omitted. Where the Response element is set to REJECT it shall take one of the following values: KEY DETAILS INCONSISTENT KEY PREVIOUSLY REVOKED SIGNATURE CHAIN INVALID AUTH ALREADY EXPIRED INVALID SIGNATURE
M	Original Request	The data in the original request (so that the signature can assure non-repudiation by the CDB)

9.13 Revoke Public Key Information Flow

9.13.1 Purpose

Used by a CP to revoke a previously registered key. This is equivalent to causing that key to expire early so that it can no longer be used. A CP/Ofcom **may**, for any reason, revoke a key held by the Central Numbering Database. The key is still available to the Retrieve Public Key Information flow.

9.13.2 Request information elements

Table 9.13.1

M/O	Identity	Notes
M	ID	Transaction Identity
M	Requesting Principal	Identity of CP sending request
M	Signing Key ID	Identity of the Key-Signing Key for the CP sending the request.
M	Signature	An electronic signature of the other information elements of this request, using the key identified by the Signing Key ID.
M	Key ID	The ID of the key derived from the key using the standard ID mechanism for that type of key.

9.13.3 Procedure

The Central Numbering Database **shall** ensure that the key signing the transaction is valid. Furthermore either**,**

a) the request shall be signed by a Root Key-Signing Key, or

b) the CDB shall validate the Key Signature chain from the key being revoked to the key signing the request.

9.13.4 Response information elements

Table 9.13.2

M/O	Identity	Notes
M	ID	Transaction Identity
M	Requesting Principal	Identity of CP sending request
M	Signing Key ID	Identity of the Key for the CDB
M	Signature	An electronic signature of the other information elements of this response, using the key identified by the Signing Key ID.
M	Key ID	The ID of the key derived from the key using the standard ID mechanism for that type of key.
M	Response	The element **shall** take one of the following values: ACCEPT REJECT
O	Reason	Where the response element is set to ACCEPT this element shall be omitted. Where the Response element is set to REJECT it shall take one of the following values: KEY DOES NOT EXIST KEY PREVIOUSLY REVOKED AUTH (The Requesting Principal does not have authority to make this request) SIGNATURE CHAIN INVALID
M	Original Request	The data in the original request (so that the signature can assure non-repudiation by the CDB)

9.14 Retrieve Public Key Information Flow

9.14.1 Purpose

Used by a CP to retrieve its public keys registered with the CDB.

9.14.2 Request information elements

Table 9.14.1

M/O	Identity	Notes
M	ID	Transaction Identity
M	Requesting Principal	Identity of CP sending request
M	Signing Key ID	Identity of the Key-Signing Key for the CP sending the request.
M	Signature	An electronic signature of the other information elements of this request, using the key identified by the Signing Key ID.
O	Attribute Requested	If specified then describes the attribute of keys to be returned, may take one of the following values: ACTIVE key not revoked and not expired UNEXPIRED key not expired VALID key not revoked
O	Key ID	If specified then retrieves the key with the matching ID . See NOTE 1
O	ParentKey	If specified then retrieves the keys that are signed directly by the key that has this ID
O	Number	If specified then retrieves the keys that are applicable for these numbers
O	Group	If specified then retrieves the keys that are applicable for this named group
NOTE 1: When present this option forces the return of information on at most one key, that being corresoponding to KeyID		

9.14.3 Procedure

The CDB shall authenticate that the Signing Key ID is valid for the CP. The CDB shall return all those keys for the CP that match the optional elements (omitted element means “any”). If the transaction is not signed by a Root Key-Signing Key, the CDB shall only return keys which are either the Signing Key ID itself , or signed directly, or indirectly, by the Signing Key corresponding to the Signing Key ID.

The CDB shall authenticate that the key is valid for the CP. If so, the CDB shall then take all the keys that have been successfully registered by the CP using REGISTER PUBLIC KEY INFORMATION and examine each of them according to the following criteria. It shall then return a response including all those keys that were not rejected (that is, it contains only the keys that passed every test).

A key K is rejected if any of the following are true:

1) The key S corresponding to the Signing Key ID is not a root key-signing key, K is not the same key as S, and K is not signed, directly or indirectly, by S.

2) The "Attribute Requested" element is specified and the status of K does not match it.

3) The "Key ID" element is specified and the key ID of K does not equal it.

4) The "Parent Key ID" element is specified, it corresponds to a key P, and K is not signed by P.

5) The "Number" element is specified, K is assigned to a number group G, and the number does not currently belong to G.

6) The "Group" element is specified and K is assigned to a different number group.

In tests (1) and (4), the validity or otherwise of any signature does not affect the results of the test.

9.14.4 Response information elements

Table 9.14.2

M/O	Identity	Notes
M	ID	Transaction Identity
M	Requesting Principal	Identity of CP sending request
M	Signing Key ID	Identity of the Key for the CDB
M	Signature	An electronic signature of the other information elements of this response, using the key identified by the Signing Key ID.
M	Response	The element **shall** take one of the following values: ACCEPT REJECT
O	Reason	Where the Response element is set to ACCEPT this element shall be set be omitted. Where the Response element is set to REJECT it shall take one on the following values: AUTH WRONG KEY TYPE
O	Key Data	If the Response is ACCEPT, a sequence of at least one Key Data element as defined below.

9.14.4.1 Key Data

Table 9.14.3

M/O	Identity	Notes
M	Key ID	The ID of the key derived from the key using the standard ID mechanism for that type of key.
M	KeyData	The public portion of the key
M	Type	Specifies the type of key that this is ROOT INTERMEDIATE APPLICATION
M	StartDate	The date and time (GMT) from which this key will become valid
M	EndDate	The date and time (GMT) at which this key will expire
O	Group	If this Key applies to a non-default Number Group then its identifier . If the Key applies to the default Number Group, then null. If the Key is CP-wide then this is omitted.
M	RevokationState	One of the values – VALID or REVOKED

9.15 List Sections Information Flow

9.15.1 Purpose

This transactions shall be used by a CP to obtain the list of Sections that are currently held in the CDB.

9.15.2 Request Information Elements

Table 9.15.1

M/O	Identity	Notes
M	ID	Transaction Identity
M	Requesting Principal	Identity of CP sending request
M	Signing Key ID	Identity of the Application Key for the CP sending the request. This must be a CP-wide key.
M	Signature	An electronic signature of the other information elements of this request, using the key identified by the Signing Key ID.

9.15.3 Procedure

A CP **shall** request a list of Sections and the CDB shall respond with a full list of the Sections within Timer T_{14} of receiving the request. The CDB shall authenticate that the Signing Key ID is valid for the CP.

9.15.4 Response Information Elements

Table 9.15.2

M/O	Identity	Notes
M	ID	Transaction Identity
M	Requesting Principal	Identity of CP sending request
M	Signing Key ID	Identity of the Key for the CDB
M	Signature	An electronic signature of the other information elements of this response, using the key identified by the Signing Key ID.
M	Response	The element **shall** take one of the following values: ACCEPT REJECT
O	Reason	Where the Response element is set to ACCEPT this element shall be set be omitted. Where the Response element is set to REJECT it shall take one on the following values: CP *(the App_key does not match the CP)* AUTH *(the App_key does not have the required privileges)*
O	Sections	Where the Response element is set to ACCEPT a sequence of at least one Section of Database as defined below

9.15.4.1 Section of Database

Table 9.15.3

M/O	Identity	Notes
M	Section	A Section of the database. This is sent as a partial number with the last digit being the C digit.
M	Quantity	The number of telephone numbers in this Section that are populated with Destination Group information

9.16 Audit

9.16.1 Purpose

This transaction **shall** be used by Ofcom to audit the CDB contents

9.16.2 Request Information Elements

The transaction request shall consist of the following parameters:

Table 9.16.1

M/O	Identity	Notes
M	ID	Transaction Identity
M	Requesting Principal	Identity of CP or Ofcom
M	Signing Key ID	Identity of the Application Key for the CP sending the request.
M	Signature	An electronic signature of the other information elements of this request, using the key identified by the Signing Key ID.
M	Start Number	The number from which audit information is required (e.g. 020 0000 0000)
M	End Number	The number to which audit information is required (e.g. 020 9999 9999)
O	CP	An optional constraint to limit data to that associated with a particular CP

9.16.3 Procedure

The CDB **shall** authenticate that the Application Key is valid for Ofcom or a CP. The CDB **shall** respond to the transaction request in the format as specified below. The returned data shall be restricted to data as follows:

- For an Ofcom key, the data relating to all CPs
- For a CP–wide key, all data relating to the CP
- For a CP key assigned to a specific Number Group, all data relating to the number group

9.16.4 Response Information Elements

Table 9.16.2

M/O	Identity	Notes
M	ID	Transaction Identity
M	Requesting Principal	Identity of CP sending request
M	Signing Key ID	Identity of the Key for the CDB
M	Signature	An electronic signature of the other information elements of this response, using the key identified by the Signing Key ID.
M	Response	The element **shall** take one of the following values: ACCEPT REJECT
O	Reason	If applicable, the element **shall** take one of the following values; AUTH *(the App_key is not valid)* CP *(if included, the CP identity wasn't valid)* NUMBER *(either the start or end number was not valid)*
O	Number Range Information	If the Response is ACCEPT the this element contains the sequence of Number Range Information elements, defined in the table below, needed to provide the information requested

9.16.4.1 Number Range Information

Table 9.16.3

M/O	Identity	Notes
M	CP	The identity of the CP with access rights to a range of numbers
M	Assigned	The quantity of numbers between Start and End Number for which the CP has access privileges
M	Routed	The quantity of numbers between Start and End Number for which the CP has populated Destination Groups

10 Timer details

10.1 Urgent changes to CDB

10.1.1 Timeline for implementation of number ports

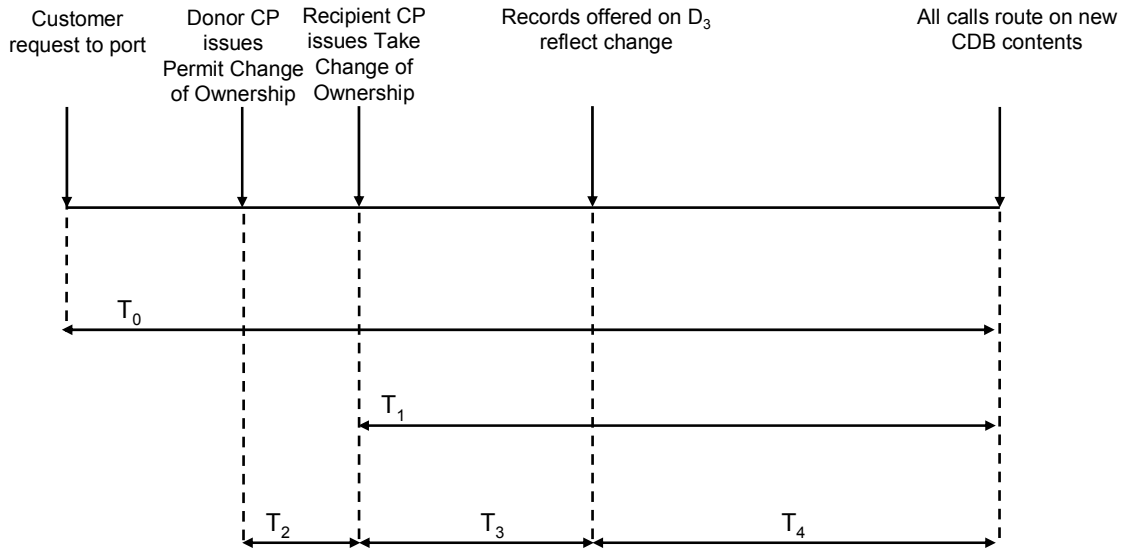

Figure 9 : Porting Timeline for real-time query scenario

NOTE : This figure assumes an implementation of the CDB in which both the real-time and bulk download functionality is incorporated, i.e. not the implementation depicted in Clause 4.3.1.3 of the present document.

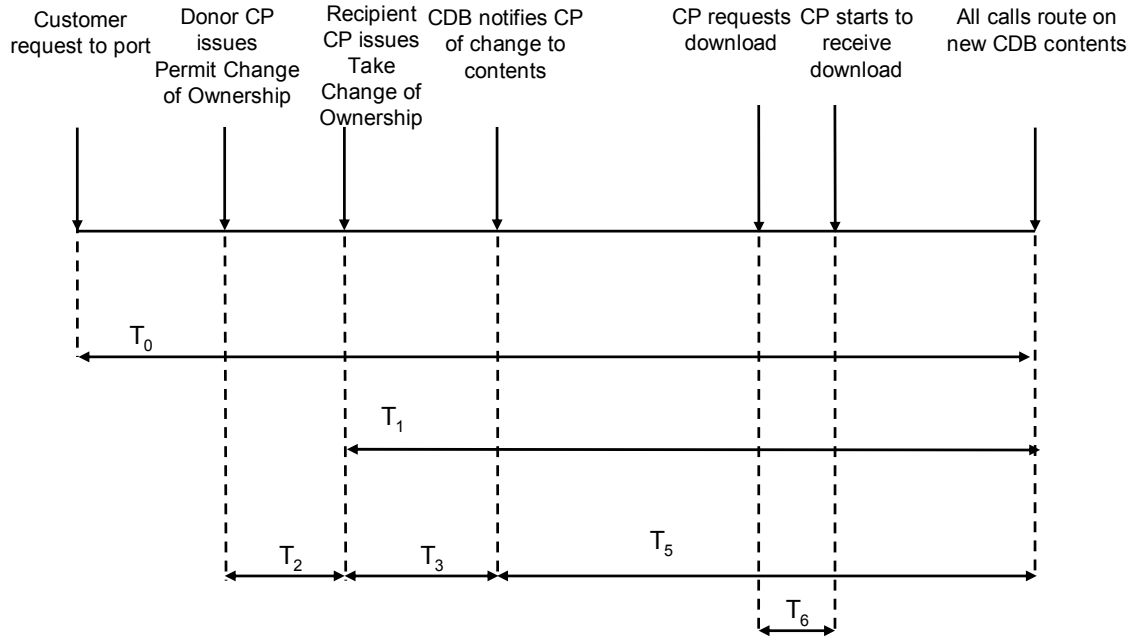

Figure 10 : Porting Timeline for reference download scenario

10.1.2 Timer Values

The following timer values **shall** apply. The timer values shall be interpreted by reference to the Clauses specified in the following table.

Table 10.1

Timing Constraint	See Clause (of the present document)	Value
T_0	N/A	Set by regulation.
T_1	N/A	Set by industry agreement: 20 minutes
T_2	9.2.3	2 minutes
T_3	4.3.1.1 8.1.3	8 minutes
T_4	4.1.2.4 8.4.4	12 minutes
T_5	4.1.1.4	12 minutes
T_6	4.3.1.1	20 seconds

NOTE: The values above must be read in conjunction with the text of the Clauses referenced. For example, for CPs value T_2 refers to the *minimum* time which must elapse after the Donor issues a Permit Change of Ownership transaction before a Recipient's Take Change of Ownership can be successfully processed by the CDB; conversely, this also means that from the CDB perspective T2 represents the *maximum* time that is allowed to elapse after a Permit Change of Ownership before it is able to process a Take Change of Ownership from a CP.

10.1.3 Other Porting-related Timer Values

The following timer values **shall** apply

Table 10.2

Timing Constraint	See Clause (of the present document)	Description	Value
T_7	9.2.3 9.3.3	Time after which a "Permit Change of Ownership" transaction will expire	56 days

10.2 Other changes to CDB

The following timer values **shall** apply

Table 10.3

Timing Constraint	See Clause (of the present document)	Description	Value
T_8	9.3.3 9.4.3	Time within which non-urgent changes must be reflected in CDB	3 days

10.3 Timer constraints to bulk download (D_1, D_2) interface

The following timer values **shall** apply:

Table 10.4

Timing Constraint	See Clause (of the present document)	Description	Value
T_9	8.1.3	Minimum period between change notifications for a given Section of the database	30 seconds
T_{10}	9.9.3	Time within which a CP should receive change notifications after requesting to do so	5 minutes
T_{11}	9.8.3	Time within which the list of servers to receive notifications should be amended	30 seconds
T_{12}	9.10.3	Time within which CDB should stop sending change notifications to a CP that unsubscribes	5 minutes
T_{13}	9.11.3	Time within which CDB should provide a list of active subscriptions	1 minute
T_{14}	9.15.3	Time within which CDB should provide a list of available subscriptions	1 minute
T_{14A}	8.3.3	Time for which data is retained in a form that can be accessed relative to a checkpoint	48 hours
T_{14B}	8.2.3	Time following the bulk download of a Section for which it is possible to update it by incremental download.	2 hours

10.4 Timer constraints on real-time interfaces

The following timer values **shall** apply:

Table 10.5

Timing Constraint	See Clause (of the present document)	Description	Value
T_{15}	4.1.1.4	Time for CP copy of CDB to respond to routeing function request	Specified by CP
T_{16}	4.1.2.3 4.3.1.2 8.4.3	Time for CDB to respond to routeing function request	20ms

10.5 Timer constraint on Data Retention

The following timer values **shall** apply:

Table 10.6

Timing Constraint	See Clause (of the present document)	Description	Value
T_{17}	4.1.2.4 9.7.3	Time which records of data in the CDB shall be kept and made available in response to query requests	(To be Advised) Years. This timer value shall be set to a value, such that users of the retained data are able to meet the regulatory requirements which fall upon them from time to time.

11 Requirements for Interfaces

11.1 B2B Interface

The B2B interface will be specified in a separate document that is specific to that protocol in which the Information flows across Reference Point M are elaborated. It is expected that design of the data structures needed is most likely to be done using XML. Consideration of the information flows in the present document will allow a set of XML schemas to be designed that implement the information elements and their associations in such a manner as to allow efficient implementation.

In the design of the protocol or profile for this application there is a need to specify general response and error codes that are required for the correct operation of the protocol but not specified in the present document. Such error codes should be in a separate name space so that application designers are clear about the nature of codes that they receive.

It may be appropriate to allow pending responses to transactions when a server is busy. The handling of such pending responses is intended to be within the B2B architecture and not visible to the Application Users. The design of the B2B Application shall be such as to permit this feature. At the Application level the user expects only to see transactions derived from the Information Flows that are accepted or rejected. Dealing with the delays that may occur at the application level is a matter for the protocol specification.

Some security services are implied by the information flows e.g. Authentication, Non-Repudiation and Message Integrity. The use of these services are described as end to end between application users by the information flows. The protocol specification may allow some of these functions to be implemented at the B2B Level however the implementation of any one model should be optional subject to an acceptable risk analysis. The specification should avoid imposing a single model of operation on all participants. Nevertheless the protocol specification shall provide full interoperability between all users irrespective of the specified implementation options that are chosen.

Nothing in the present document shall prevent the framework (Automated Business to Business (B2B) Transactions: Architecture and Principles) [2] and NICC ebXML profile [3] being used in conjunction with this specification. However only one protocol is to be used for the B2B interface in compliant implementations and that will be described in another specification that refers to the present document as its source of requirements.

The signatures process used for digital signing of messages should be based on a known robust end to end digital signing process

11.2 Protocol Implementation of D_1, D_2 and D_3 Reference Points

A protocol which is used to implement the D reference points shall include mechanisms to handle lost messages, whether requests or responses, by means of retries. The time between retries and the number of retries before a peer is

deemed unserviceable is a protocol design matter. Consideration should be given to attempting automatic return to service when peers have become unserviceable.

Annex A (normative): Record Formats for the Common Database

A.1 Introduction

The common database will contain records of three forms, known as the "PSTN form", the "IMS form" and the "SEND-N form".

- Where a number is served by a PSTN call model (whether traditional TDM or PES on an NGN), the database will only contain records of the PSTN form.
- Where a number is served by an IMS network, the database will contain records of both the PSTN and IMS types, unless the nature of the service is such that interworking via PSTN is not possible, in which case it will contain records only of the IMS type.
- The SEND-N form is used to indicate valid prefixes that aren't complete numbers.

A.2 SEND-N form records

SEND-N records are used when a too-short number is looked up, and indicate the minimum number of digits that would be required to create a valid international E.164 telephone number.

SEND-N records SHALL be provisioned in the central database, generated automatically based on the numbers that have been provisioned. The use of SEND-N records by CPs is optional.

A.3 URIs

Syntax in this document uses ABNF as defined in STD 68 [7] including appendix B. Note that quoted strings are case-insensitive but SHOULD use lower-case.

The overall syntax is:

```
database-uri = tel-uri / sip-uri / send-n-uri
```

A.3.1 PSTN form records

The URI generated by the records **shall** be of the form:

```
tel-uri = "tel:" PSTN-group UK-number ";phone-context=+44"
PSTN-group = "7" CP-identity internal-destination
CP-identity = ("2" / "3" / "4" / "5" / "6" / "7" / "8" / "9") 3DIGIT
internal-destination = 3DIGIT
UK-number = "0" 7*10DIGIT
```

The PSTN-group defines a Destination Group as described in Sub-Clause B.2.

For example:

```
"tel:7333344401234567890;phone-context=+44"
```

Note that the UK-number includes the leading zero and that the only parameter permitted is "phone-context" (the *tel* URI is formally described in RFC 3966 [6]).

Records in the common database MUST NOT use the PSTN-group 72000000.

CPs **should** arrange their values of internal-destination to be aggregatable for routeing purposes.

A.3.2 IMS form records

The URI generated by the records **shall** be of the form:

```
sip-uri = “sip:” UK-number “@” IMS-group
IMS-group = CP-IMS-group “.dg.” CP-label “.uktel.org.uk”
CP-IMS-group = label *(“.” Label)
CP-label = label
label = LD [*61LDH LD]
LDH = LD / “-”
LD = ALPHA / DIGIT
```

The IMS-group defines a Destination Group as described in annex B.3.

For example:

```
“sip:01234567890@cs23.posi073.dg.example.uktel.org.uk”
```

Note that no URI-parameters are permitted (the *sip* URI is formally defined in section 19.1 of RFC 3261 [5]).

A.3.3 SEND-N form records

The URI generated by the records will be of the form:

```
send-n-uri = “pstndata:send-n/” length-information
length-information = number
number = NZDIGIT [DIGIT]   ; 1 to 99, no leading zeroes
NZDIGIT = %x31-39          ; 1 to 9
```

For example:

```
“pstndata:send-n/12”
```

•

The number indicates the minimum number of digits required to make up a valid international E.164 telephone number. It makes no assertion about the maximum.

Note : A subsequent version of the present document may change the exact syntax of the URL to bring it into alignment with international standardisation activity.

As an example of the SEND-N records, suppose that all 0888 numbers are either 11- or 12-digits (replacing the leading zero with the country code "44") and, in particular, numbers in the range 0888 55566x are all 11-digit while those in the range 0888 55577xx are all 12-digit, then the URIs generated by the SEND-N records would be:

```
+448885         pstndata:send-n/11
+4488855        pstndata:send-n/11
+44888555       pstndata:send-n/11
+448885556      pstndata:send-n/11  ; there could be 0888 555 6xxx 12-digit numbers
+4488855566     data:send-n/11      ; but all 0888 55566x numbers are 11-digit
+448885557      data:send-n/11      ; there could be 0888 5557xx 11-digit numbers
+4488855577     data:send-n/12      ; but all 0888 555 77xx numbers are 12-digit
+44888555770    data:send-n/12
+44888555771    data:send-n/12
; ...
+44888555779    data:send-n/12
```

NOTE: When the CDB synthesises SEND-N form records a number is taken into account only if it has PSTN or IMS form records associated with it. In other words, "valid" in the above description actually means "valid and with a record provisioned in the CDB".

Annex B (normative): Destination groups

B.1 Introduction

A key concept for the common database and the records therein is the "destination group". The purpose and reasoning behind these is explained in other documents but, briefly, a destination group represents the set of all numbers which all CPs – other than the one hosting them – would expect to route in an identical manner. The present annex is only concerned with the syntax of destination groups.

B.2 PSTN destination groups

For PSTN form records, a destination group is divided into three components:

1. the prefix, which is always the digit 7;
2. the CP-identity, which identifies either an individual or group of CPs and is a four-digit number between 2000 and 9999 inclusive, allocated centrally;
3. the internal-destination, which identifies either a location within a CP, or a CP within a group of CPs, and is a three-digit number retaining leading zeroes, i.e. in the range 000 to 999.

This form of destination group thus falls into the UK numbering plan in an empty space (codes beginning 7 are "targeted transit" but Ofcom has agreed that 70 and 71 will suffice for this). On a per-CP basis, it is intended that either

- a CP will be assigned a CP-identity by a central authority and will then be able to allocate 1000 different destination groups using that identity. Should a CP require more than this number, a second or subsequent identity can be allocated to them. Or,
- a group of CPs will be assigned a common CP-identity by a central authority and each CP within that group will be assigned one or more internal-destination values. For example, number-length constraints in existing mobile solutions mean that it isn't feasible for mobile networks to support multiple destination groups, so mobile networks will share a common CP-identity as described in clause B.4.

B.3 IMS destination groups

For IMS form records, the destination group is a domain name conforming to ND1633 [1], made up of four components:

1. the <*network internal part*>, which is an arbitrary sequence of labels;
2. the <*local application ID*> label "dg", to indicate that this is a destination group;
3. the <*provider*> label, which is a label allocated in accordance with ND1633 [1];
4. the NGN root domain "uktel.org.uk".

The arrangements for notifying other CPs about valid destination groups, and the routes to use for traffic, are to be agreed bilaterally.

B.4 Special purpose CP-identities

The CP-identities 2000 to 2099 are reserved for standardisation purposes and MUST NOT be allocated to CPs. The following values are used at present.

7 2000 000 This is the "default destination group" and is used to indicate that a number was not found in the common database.

7 2007 XXX The CP-identity 2007 is assigned collectively to those CPs providing mobile service using 07 numbers. Using a destination group of 72007PQR is identical in effect to using the mobile number portability Mobile Routeing Code 07PQR (that is, 72007PQR07ABCDEFGHJ is identical in effect to +447PQRABCDEFGHJ) but fits into the destination group schema. The only values of Mobile Routeing Code that may be used are those allocated by Ofcom for this purpose (such as 617 or 992). As such this requires that Ofcom ensures the allocation of Mobile Routeing Codes is continued to cover all future new mobile entrants' requirements for direct routeing using the CDB. This will ensure this solution is future proofed.

7 2099 XXX These destination groups are for internal use by a CP and MUST NOT appear on interconnects. They MUST NOT appear in the common database. It may be desirable in the future for all the 209X identities to be used for this purpose, and so the CP-identities 2090 to 2098 should not be used for other standardisation purposes at present.

Annex C (normative): Routeing Logic

C.1 Introduction

Within the present Annex, notes are included for explanatory (non-normative) purposes.

There are five basic situations to consider.

1. The incoming called number is provided in the CPN element of an ISUP message. This is described as "PSTN" in the present Annex.
2. The incoming called number is provided via SIP in a *tel* URI not as part of an IMS service. This is also described as "PSTN". In accordance with section 19.1.6 of RFC 3261 [5], a URI of the form "sip:1234;phone-context=uktel.org.uk@example.com;user=phone" – where the user component would be a valid tel URI (apart from the scheme) and there exists a "user" URI parameter with the value "phone" – is equivalent to a tel URI for the purposes of the present Annex.
3. The incoming called number is provided directly to an IMS service from an originating user agent. This is described as "IMS-OUA".
4. The incoming called number is provided via SIP in a *sip* URI of the form specified in Annex A of the present document. This is described as "IMS-SIP".
5. The incoming called number is provided via SIP as part of an IMS service in a manner not covered by the previous cases. There must be a bilateral agreement between this node and the one connecting to it that enables the number and any prefix to be located within and extracted from the incoming URI). For example, current IMS implementations use a URI of the form "sip:0123456789@host.example.net"; if it is agreed that this form will be used, the number is unambiguously the part before the @ sign. This is described as "IMS-TEL".

The architecture is designed to prevent calls between networks from requiring number translation queries in more than one network. Therfore NGNs using this architecture prevent there being translation queries in interconnected networks to which calls are conveyed. This is sometimes described colloquially as a requirement for only one database dip per call. That colloquial description is imprecise because nothing in the architecture is intended to prevent any given CP from using data translation queries any number of times within its own network. It is also the case that in a limited number of cases more than one translation queries will be needed e.g. in interworking between PSTN and IMS services.

C.2 Description of Routeing Logic

There is a flow diagram at the end of this Annex.

This routeing algorithm consists of a number of steps. The process starts at the initial step; it and all other steps end by a jump to another step or by terminating the call, failing it, or sending it on to another node. The steps, in the order they are found in the present Annex, are:

Initial step

Step DD (routeing requiring a database dip)

Step NE (no entry in the database)

Step NR (routeing based on number range)

Step TU (routeing based on a *tel* URI from a database dip)

Step RP (routeing based on a *tel* URI containing a 7xxxxxxx destination group or a 5xxxxx number portability prefix)

Step SU (IMS routeing based on a *sip* URI from a database dip)

Step SR (IMS routeing based on a *sip* URI)

Step CO (outbound management)

Step IO (IMS outbound management)

Step PO (PSTN outbound management)

Note that an implementation need not simulate these steps, or any part of them, providing that it has the same behaviour as this algorithm would produce.

Initial step

The following rules apply to the destination information that is to be analysed:

Only one prefix can validly be put on a number, therefore it is not necessary to consider the situation where there are two prefixes.

An incomplete number can have the default destination group 72000000 but no other prefix.

The only valid format for a sip URI in the IMS-SIP case is one containing a destination group and no prefix.

Since the prefixes are non-diallable, the IMS-OUA case cannot include prefixes

Examine the destination information:

Table C.1

Nature of Result	Action			
	PSTN	IMS-SIP	IMS-OUA	IMS-TEL
Contains default DG	→NR	n/a	n/a	→NR
Contains any other DG	→RP	→SR	n/a	→RP
Contains NP prefix but no DG	→RP	n/a	n/a	→RP
Contains no DG or NP prefix	→DD	n/a	→DD	→DD
NOTE: n/a = not applicable				

NOTE: in appropriate circumstances (the definition of which are outside the scope of the present document), if an operator routinely processes IRNs and if the prefix is in the 72007xxx group, then the operator may wish to replace it and the leading 07 of the number with the corresponding 07xxx IRN.

NOTE: If there is a real destination group or number portability prefix on the number, this definitely identifies the final destination and so should be used for routeing, ignoring anything else. If the default destination group is on the number, a database dip has already taken place with no result; therefore the call must be routed on the basis of number block. If no prefix is present, the node should do a database dip.There cannot validly be more than one prefix on a number.

NOTE: (Rationale) The “n/a” cases occur for IMS-SIP because the only valid format for these sip URIs is one containing a destination group and no prefix. For IMS-OUA, they occur because the prefixes are non-diallable and so cannot appear in the presented number.

Where the number begins with a mobile porting prefix (e.g. 07617 or 07992), the node MAY treat it as either a special form of NP prefix or as an ordinary number without prefix.

Step DD (routeing requiring a database dip)

Query the database:

Table C.2

Nature of Result	Action			
	PSTN	**IMS-SIP**	**IMS-OUA**	**IMS-TEL**
both *sip* and *tel* URIs	→TU	n/a	→SU	→SU
sip URI only	→NE	n/a	→SU	→SU
tel URI only	→TU	n/a	→TU	→TU
neither type of URI present	→NE	n/a	→NE	→NE
NOTE: n/a = not applicable				

In the case of PSTN with only a sip URI in the database, this indicates that the number is served by IMS but not PSTN. The node MAY check for sip URIs when doing a query in the PSTN case. If it does check and finds only a sip URI, it MUST fail the call at this point. If it does not make the check, it will find no URIs for the number and will progress to step NE.

NOTE: (Rationale) If a record is found in the database, its type and contents will determine the subsequent behaviour; the different jumps in this table are chosen so as to correctly apply the rules of precedence (*sip* before *tel*, but only for IMS cases). In steps SU and TU the results of the dip will override any existing routeing.

NOTE : (Rationale) The IMS-SIP case never reaches this step.

NOTE: (Rationale) By definition in Annex B of the present document, a tel URI in the database is for PSTN working and a sip URI is for IMS working. Neither can contain the default destination group 72000000 or a number portability prefix.

NOTE: If a SEND-N response is received, either the appropriate additional digits should be collected and the routeing logic restarted from the initial step, or the call should be failed.

Step NE (no entry in the database)

Prefix the default destination group to the number, then →NR.

NOTE: The call will be routed based on number range, but with the default destination group added to prevent a second database dip.

Step NR (routeing based on number range)

Analyse the destination number range (ignoring the default destination group):

Table C.3

Hosting Node	Porting State	Action
Node hosts the range:	number is ported out:	replace the default destination group with the appropriate 5xxxxx number portability prefix, 7xxxxxxx destination group, or 07xxx IRN (which will require removing the initial 07 from the number), determine the next hop using that prefix, then →CO;
Node hosts the range:	number is not ported out:	terminate the call.
Node does not host the range (See NOTE 1)	any	determine the next hop using the number range, then →CO. The node should not remove the default Destination Group.
NOTE 1: It is possible that the node does not host this number range but does host the called number because it has been ported to it. The node SHOULD check for this situation and terminate the call directly. If it does not, the call will eventually be tromboned back to this node with a DG or NP prefix attached to the number.		

NOTE: This is traditional routeing: terminate the call if this is the destination, use the number range to determine the next hop for outward calls, or add the 5xxxxx prefix for ported numbers and route based on that. While it is unlikely that a 7xxxxxxx prefix would be used in this situation, it is not forbidden.

NOTE: The default prefix should be retained on the number so that the next node to process the call does not need to make a second dip of the database. If the prefix is stripped, this will cause a second dip but cannot result in circular routeing of the call (although in some circumstances it may be tromboned). If the common database is not fully consistent, the call may terminate at the wrong node and thus fail but, if so, this would also apply to calls to the same destination where this node is the first one to dip the database.

NOTE: If the number range is unallocated or otherwise has no route, the call should be failed. If the number is incomplete and not long enough to determine a unique next hop, either the appropriate additional digits should be collected and the routeing logic restarted from the initial step (using the prefix, if any, it carried on arrival), or the call should be failed.

Step TU (routeing based on a *tel* URI from a database dip)

Replace the called number by that (including prefix) in the *tel* URI retrieved from the database. Finally → RP.

NOTE: in appropriate circumstances (the definition of which are outside the scope of the present document), if an operator routinely processes IRNs and if the prefix is in the 72007xxx group, then the operator may wish to replace it and the leading 07 of the number with the corresponding 07xxx IRN.

Step RP (routeing based on a *tel* URI containing a 7xxxxxxx destination group, an IRN or 5xxxxx number portability prefix)

Analyse the prefix: (7xxxxxxx destination group, 5xxxxx number portability prefix, or 07xxx IRN)

Table C.4

Prefix Hosting State	Number Hosting State	Action
Node hosts the DG or NP Prefix:	node hosts the number	terminate the call
Node hosts the DG or NP Prefix:	node does not host the number	fail the call – data out of sync
Node does not host the Prefix See NOTE 1)	any	determine the next hop using the number range, then →CO.
NOTE 1: While a number port is taking place, inconsistencies in cached data could mean that the node hosts the called number even though it does not host the DG or NP prefix specified. The node MAY check for this situation and terminate the call directly; if so, it SHOULD report that there is a data synchronisation problem. If it does not, the call will eventually either get failed elsewhere or delivered to the line hosted by the node hosting the DG or NP prefix.		

NOTE: (Rationale) If the number begins with a prefix then that, rather than the number range, controls routeing. If it is one of the prefixes hosted by this node, the call definitely terminates here – this can only happen if either this node's DG appeared in the common database or the Donor Operator applied a prefix allocated to this node and Onward Routed

NOTE: This step MAY also be used with IRNs if the node chooses to treat them as routeing prefixes rather than ordinary numbers – see the initial step..

Step SU (IMS routeing based on the destination group in the host part of a *sip* URI from a database dip)

Replace the incoming URI or called number by the *sip* URI retrieved from the database, then →SR.

Step SR (IMS routeing based on the destination group in the host part of a *sip* URI)

Analyse the destination group in the URI:

Table C.5

DG Hosting State	Number Hosting State	Next Hop, from destination group	Action
Node hosts the DG:	Node hosts the number		Terminate the call
Node hosts the DG:	Node does not host the number		Fail the call – data out of sync
Node does not host the DG:		SIP NGN	send using the sip URI
Node does not host the DG:		SIP-I NGN or TDM	extract the number from the URI, interwork to PSTN, and →DD (using the PSTN column)

NOTE: (Rationale) The DG came from the common database and is therefore correct. If this node doesn't host the group, the call is forwarded. If the next hop doesn't speak SIP, extract the number from the sip URI (it won't contain a prefix), interwork to PSTN, and re-dip the database

Step CO (outbound management)

Recall the incoming connection type:

Table C.6

Connection Type	PSTN	IMS-SIP	IMS-OUA	IMS-TEL
Action	→PO	n/a	→IO	→IO
NOTE: n/a = not applicable				

NOTE: (Rationale) This step happens when we are routeing by some form of number, not a *sip* URI (and thus this step is never reached by IMS-SIP).. The next hop has already been identified and we just need to know whether or not we can use IMS and a *sip* URI (with a format agreed bilaterally) to talk to it.

Step IO (IMS outbound management)

Determine the type of the next hop:

- IMS-TEL allowed:send using a URI of the agreed form with the prefix and number.
- Otherwise: interwork to PSTN and →PO.

NOTE: Use IMS if we can that is, if there is a bilateral agreement in place for representing the number within SIP, as described in case 5 of the introduction. Otherwise we have to abandon IMS and move to PSTN.

Step PO (PSTN outbound management)

Determine the type of the next hop:

- NGN: send using *tel* URI with prefix and number;
- TDM: send using CPN with prefix and number.

Flow diagram

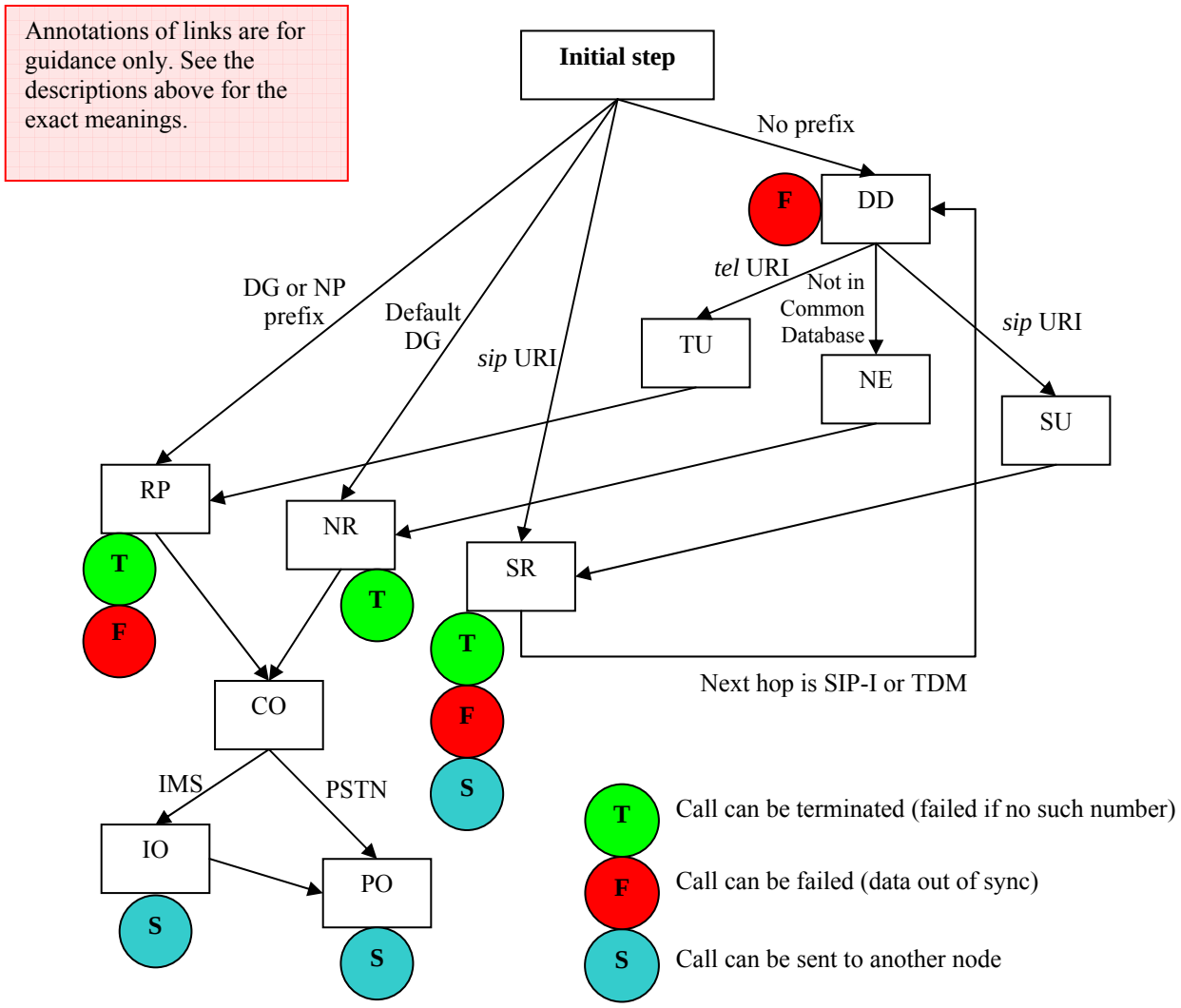

Figure C.1 Flow of routeing logic

History

Document history		
<Version>	<Date>	<Milestone>
1.1.1	2008-04-11	Initial issue
1.1.2	August 2008	Reference to ND1610 release sheet added
1.2.1	December 2008	Updated to reflect changes agreed during UKPorting negotiations (multiple notifications within single message, multiple downloads in single message, "potted" bulk download approach, changes to Send-N, bootstrapping transactions) and to add warning that regulatory changes have been set aside.
1.2.2	December 2010	Warning regards regulatory status updated