NPU-Registry

Maintenance system for mobile and fixed number portability and personal numbers

System Description Document

Version: 2.1
Date: 01-December-2015

Table of contents

1. Introduction

1.1. Definitions & Glossary of Terms

The following terms and abbreviations are used in this document:

Administrator – the company-hoster of the NPU-Registry system

Administrative rights – the permission of access level to NPU-Registry functions that can have and must have system admins only.

Customer – entity that issued the RFP of "Administrative and Technical Requirements"

Donor – it is mobile network Operator from which the subscriber's number is now porting or has been ported

Recipient – it is mobile network Operator which has gained the ported number

Subscriber – Abonent of the Telco who wants ported own number

NRA – National Regulatory Authority

Telco – telecommunication operator that supports and carries out number portability processes as participant of the NPU-Registry

1.2. General

The document describes the properties and parameters of the Number Portability Central Database System NPU-Registry v.2.0 (hereinafter – NPU-Registry) based on a central database the ported subscriber's numbers. This system has brand name NPU-Registry and has protection of intellectual property in accordance with legislation of Ukraine.

1.3. Abstract

This document describes:

1) general technical architecture and subsystems of NPU-Registry;
2) functions of the subsystems;
3) software and hardware;
4) structure of the electronic forms number portability applications;
5) structure and set the NP CDB tables and files for synchronization processes between local DB of operators and NP CDB;
6) informative links in the processes of the registration and processing of electronic forms number portability applications application;
7) data processing algorithms for the all relevant to number portability procedures;
8) exchange an information messages during processing the number portability applications[1];

[1] Subject to the final processing after agreement with UNAOC.

9) sequence of actions during processing applications[1];
10) the processes of xml-structures formation for EPP-commands and EPP-extensions according to RFC5730 Extensible Provisioning Protocol (EPP).

1.4. Overview

System NPU-Registry has been designed to manage the processing of electronic forms number portability applications and processes of portability in their capacity as such.

System NPU-Registry allows to operate with options relating to the management of personal numbers and non-geographic numbers including codes of nomadic numbers.

System NPU-Registry generates the data flows that allow managing the processes of number portability for VoIP.

The electronic forms number portability applications are designed as three types:

1) initiate the number portability of subscriber numbers,
2) refuse of the number portability process, and
3) return number to the Donor.

In the base configuration, the NPU-Registry have settings on scheme “start porting from Recipient”, however might be configured on scheme “start porting from Donor”.

The system can be settings on servicing of the individual users, corporate users, institution users as well as contract and pre-paid users.

NPU-Registry can adapt to various configuration:

1) with NP Central Database (CDB) of the Administrator and NP Local Database (LDB) of the Telcos;
2) with NP CDB of the Administrator only and without NP LDB of the Telcos.

NPU-Registry can process:

- mobile and fixed ranges of the subscribers’ number in any technological environment of the PSTN/PLMN;
- personal subscribers’ numbers and support Registry of the personal subscriber numbers according to range in the national numbering plan;
- non-geographic and nomadic number portability on requests of the Telcos networks;
- and integrate during the portability the VoIP numbers when receive a call request from the telecommunication network;
- geolocation functionality;
- and support the portation with saving all the set services that has subscriber in the Donor network.

2. The architecture and functionality of the software and hardware

2.1. Functionality of the subsystems

2.1.1. Components of functional structure

Functional structure of the NPU-Registry includes the components:

1) Number portability central database (NP CDB);
2) Subsystem of the interfaces;
3) Subsystem of the analysis and automatic handling of the new number portability applications;
4) Subsystem decision-making according to the rules of processing of applications that been received
5) Subsystem of the auditing and analytical;
6) Subsystem of the administration;
7) Monitoring and Help Desk subsystem;
8) Subsystem of cryptographic security (implementation depends on national legislation);
9) WHOIS service (optional).

Functional structure of the NPU-Registry v.2.0 shown on Figure 1.

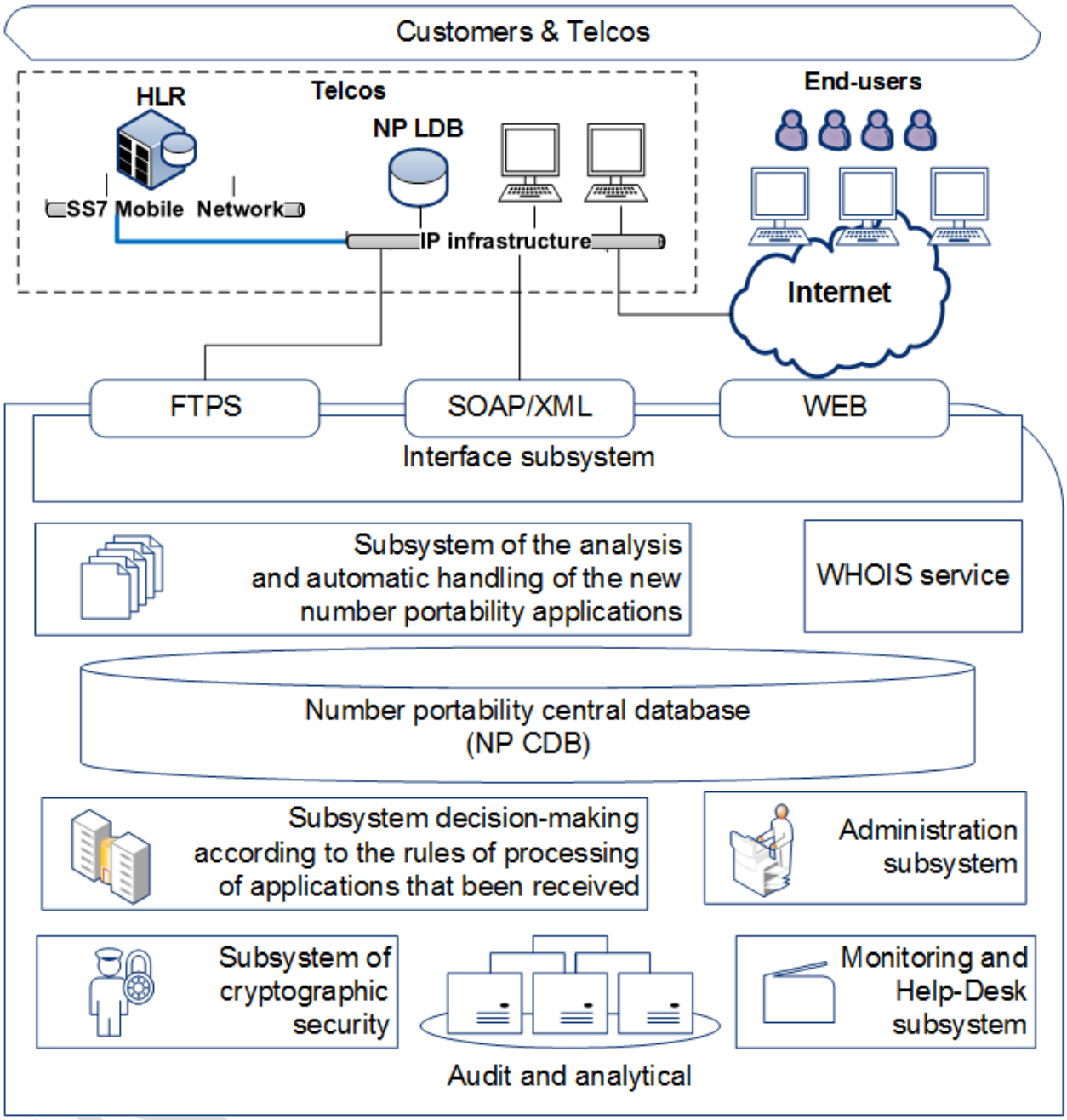

Figure 1. Functional structure of the NPU-Registry v.2.0

2.1.2.Operation modes

Operation modes provides interoperability of the NPU-Registry subsystems and ensures:

- continuous operation 24*7*365;
- reliability and service availability not less than 99,9%;
- processing applications to portability in quantities and relevant minimum bandwidth not less than 500′000 per hour;
- invariance with respect to the implementation of the number portability model by operators;

- maintenance of all operators operating at the time of the system implementation and possibility of increase their quantity without major technical changes;
- storing information about all subscriber numbers that have been allocated to the telecommunications operators according the National Numbering Plan;
- the ability to administer at least 50'000'000 ported numbers with the possibility of increasing their quantity without any significant technical changes;
- storing data arrays about number portability history not less than 5 years;
- processing duration of the exchange messages operations between NPU-Registry and operator networks during number portability process not more than 1 hour in online mode and not more than 1 day in offline mode;
- flexible configure parameters of the NPU-Registry.

The NPU-Registry functionality is aimed at flexibility and adaptability to the specific requirements and demands of the Customer for setting up decision-making processes:

- decision-making in accordance with Customer's criteria for permitting or rejecting/cancelling a porting request;
- simultaneously support multiple number portability processes with possibility of the distribute the ones on participants;
- transferring data between clusters of the NPU-Registry and confirmation of receiving ones;
- formation and maintenance the structure and sequence of messages indicating the relationships between requests and responses;
- confirmation automatically of the each received request on validity of the number portability application according to certain Customer's criteria, and specifying the error codes;
- administration of the portability of geographic, non-geographic, and nomadic numbers;
- returning number (s) to the Donor in the case when the user cancelled the contract with the Recipient (the event conditions should be configured according to national legislation).

In the basic variant the NPU-Registry don't carry out the routing between operators networks; the support number portability applications and maintenance central database only.

However, the NPU-Registry system have additional extension and can be sets to the options that provides the routing of voice calls between subscribers or delivery SMS and MMS.

NPU-Registry can process non-geographic and nomadic number portability requests to operators' networks.

NPU-Registry can process VoIP number portability request to operators'

networks.

2.1.3.Cryptographic data protection

Within the scope of the NPU-Registry implementation the basic approach to cryptography is proposed.

All cryptographic options must be localized under Customer's country legislation in effect.

Cryptographic data protection provides:

- creation pair of keys (a public and private) by Donor;
- sending a public key for certification in certification center;
- encryption of personal data;
- interconnection between the PN CDB cluster and operators' clusters;
- fixing the fact of encrypted communication session;
- decrypting the personal data using the private key;
- confidentiality and integrity of the traffic exchange between the PN CDB and LBD beginning with L3 (in accordance to the OSI model).

2.2. Software architecture

The software has the modular and the cluster architecture that includes the server part, the client parts, and the possibility of building a private and secure sessions. These sessions will be constructed from the Customer' computers and will be used for the data input in system.

The Administrator and Telcos clusters are separated. The data exchange between clusters takes place in the protection mode in accordance to security requirements for confidentiality and integrity of traffic. For the implementation of data security the system applies the means on the channel level, network routing, organizing sessions and software applications.

Filling client’s forms of the number portability applications performed through the web-server.

The system uses the software that can implemented any diagnostic answers and any queries in the languages of the country of the implementation[2].

Storing data of the number portability applications provided on a separate server before they are sent to Telcos for processing. Data transmission is carried out using the protocol FTPS (https://tools.ietf.org/html/rfc2228 and https://tools.ietf.org/html/rfc4217). The files format is .xls or .csv.

The processing-data unit and business-logic unit are located in the back office of the NPU-Registry without the possibility of access of any end-user that do not

[2] English can be in addition included.

have Administrative rights.

Software architecture is shown in Figure 2.

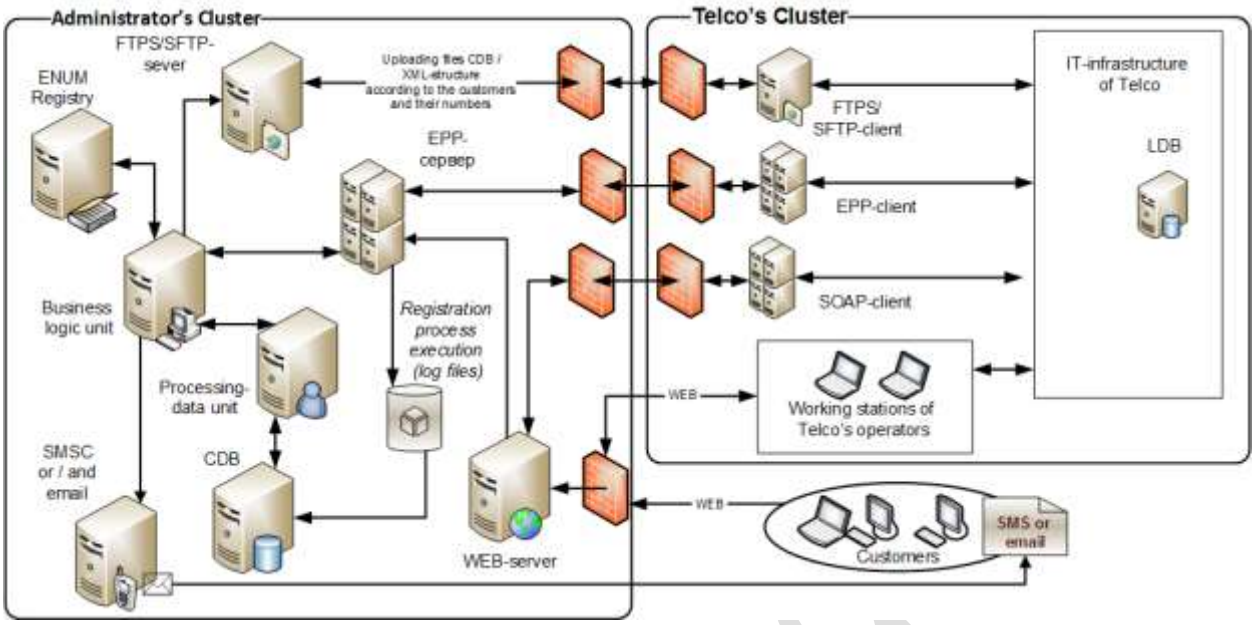

Figure 2. Figure of the software architecture

The system supports and provides functional decisions during processing of number portability applications:

1) servicing and handling of few subscriber' numbers or number range that can be specified in number portability application
2) cancellation mode by the Recipient the porting one or more numbers listed in the number portability application of a group of numbers
3) checking mode and approval or refusal of the decision from the hand of the Donor and / or Recipient during processing the porting one or few the numbers listed in the number portability application
4) mode of returning of the number to Donor
5) sequential actions on deactivation and / or activation of the ported numbers in accordance with the application.
6) ability to identify and specify the porting time by the Subscriber.
7) mode of the multi-level access and control user access in accordance with their rights and roles. The quantity of users that can operate simultaneously with the processing of number portability applications may be not less than 4096. This users' quantity can be limited and depends on the channel bandwidth and equipment processing capacity.

The upgrade of the system program code does not lead to:

1) changes of the terms as well as during current processing of the number portability applications or have been accepted ones before the upgrade:
2) interruption of system work.
3) performance degradation of system.
4) impact on the quantity of numbers and number portability applications that

can be processed.

The system provides the possibility of rejection of the latest changes in the code and fallback to the previous version via backup mechanism without stopping the process of providing the service. The system provides the possibility of support for the two versions of the same process of number portability - old for applications filed prior to the change version and new for applications filed after version changes.

For all the key components of the hardware-software complex system using the serial system software (operating systems and database software) of the industrial level ("carrier grade", "enterprise").

This is done to ensure high reliability and stability of the system.

The type of servers' and DBMS software - licensed or open source - depends from Technical Requirements of Customer. The system has not restrictions regarding the use of the types ones.

The licensed software of the system is carried out under relevant licenses..

2.3. Testing and monitoring

The system provides the possibility of testing the process of including new Telcos and step-by-step testing of the number portability process in automatic mode. All operations including erroneous are logging.

Testing of new connections to the system is carried out without any interference or influence on the work of the system production units.

The main unit, which provides testing, is located on the Administrator' site. This is due to the need to quick responding to settings of the software configuration and / or server hardware that are tested.

2.4. System architecture

The system has full redundancy of all software and hardware units and interfaces. The minimum backup is done by replacing the 1 (main unit/node/interface) + 1 (redundant block/node/interface) in hot swap mode. The system provides scalable backup units/sites/interfaces.

The productive capacity of the backup segment is not less than the main segment and provides the ability to make upgrades to the system configuration without interruption of service.

The system has two opportunities to work with clusters of Telcos - the production segment and the test segment of the Telcos.

The scheme of the system architecture shown on Figure 3.

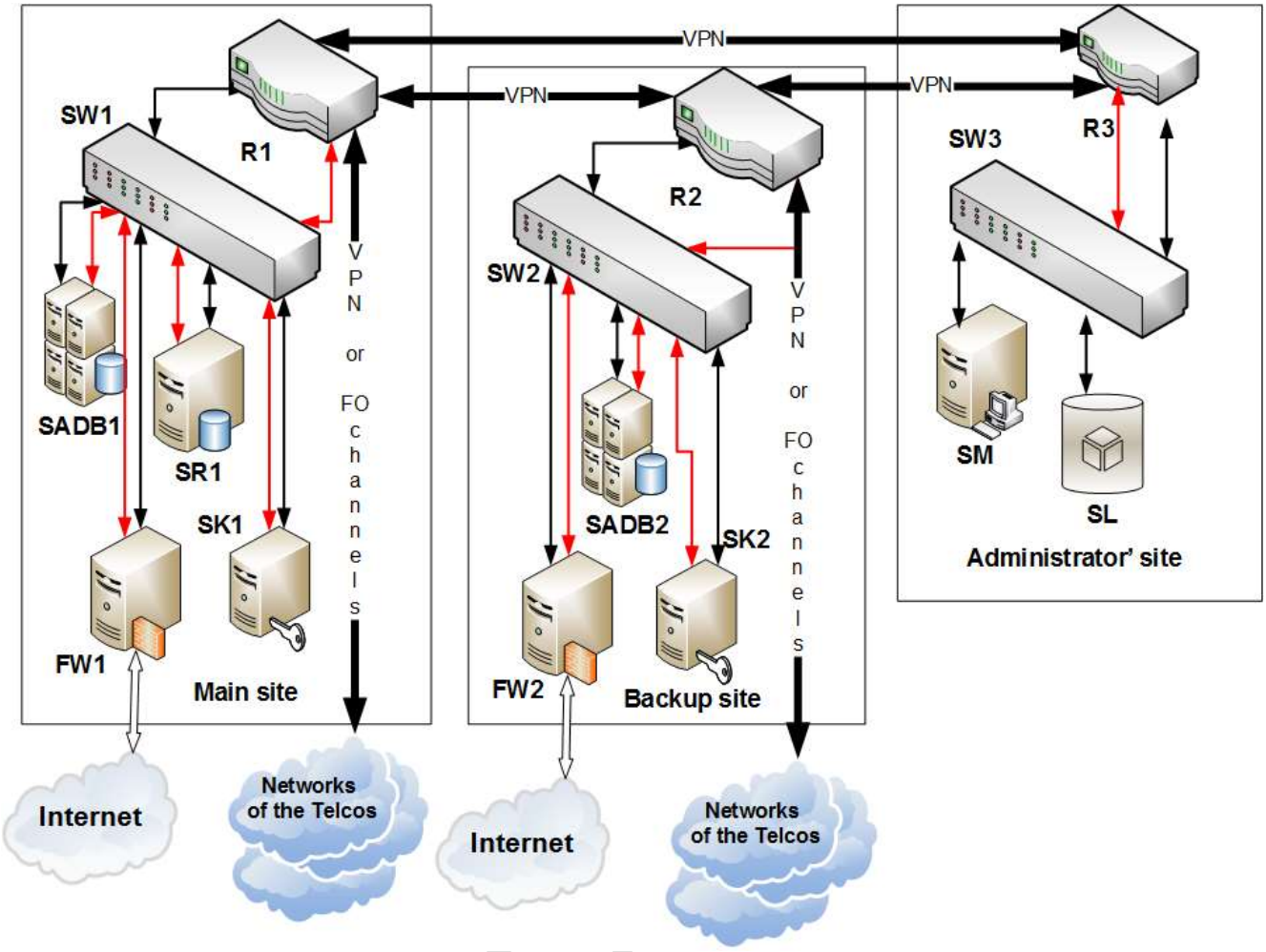

Figure 3. The scheme of the system architecture

Legend to Figure:

Black lines links – the main links within system,

Red lines links – the backup links within system,

R(i) – the routers,

SW(i) – the switches,

SABD(i) – the servers of the software applications and NP CDB,

SK(i) – the crypto servers,

SR1 – the backup server and CDB backup function,

SM – the monitoring server,

SL – the logging server.

2.5. Redundancy scheme and disaster recovery plan

All networking equipment are purchased in quantities of (N + 1) for the organization of quick replacement in case of failure of any unit.

If this equipment can not be delivered for some time on the failure technical site, the redundant units will performs in Standby mode the relevant functions as long as would be delivered. The terms of delivery according requirements and standards of Administrator must be agreed.

The redundancy scheme of the system shown in Figure 4.

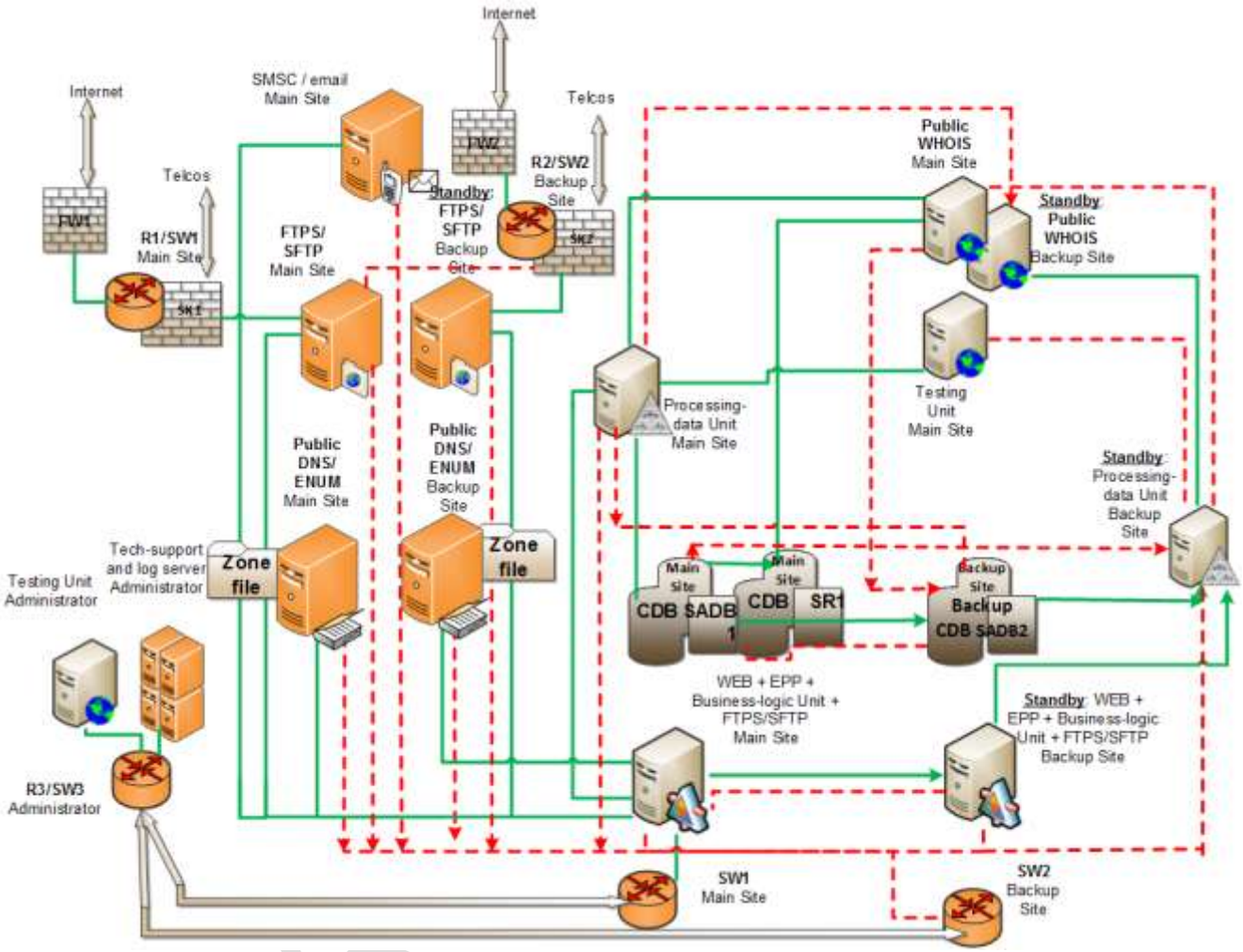

Figure 4. The redundancy scheme

functioning of the main links between elements of the system

functioning of the backup links between elements of the system

The scheme is shown in the minimum solution of the hardware system configuration.

The scheme does not reflect the physical blocks but the logical functions that perform the units (logical units). Depending on the processing capacity of the equipment, the logical units may be combined in one or several separated physical sites.

Not allowed the location the same physical site logic units that perform the main and backup functions.

Restore the system in case of accidents and emergencies is described in the document "Disaster Recovery Plan (DRP)". The DRP contains the regulations depending on the 3 levels of emergency:

1) Yellow level – are the insignificant accidents, do not lead to significant results the loss of system efficiency. These situations are characteristic for the local accidents within a single data center and can be liquidated quickly. Recovery is the result switching to the redundant units. Recovery time performance should not exceed 5-10 minutes.
2) Orange level - are the emergencies that could lead to significant consequences for the system efficiency. These situations are characteristic for the local regional accidents; the period of liquidation depends on external factors related to the violation of energy supply, the inability to maintain the temperature. Recovery is the result supporting of the emergency power supply mode, the involvement of additional sources, switching to redundant units.
3) Red level - are the emergencies related to the physical destruction of the data centers building or/and communication channels/lines as a result of a fire, natural disasters. Recovery is the result switching to the redundant power sources and deployment of the new sets of system hardware and software.

2.6. The functional parameters of the system

No.	The functional parameters of the system	Value
1	Quantity the requests on number portability that system can handle during 60 minutes, not less than	500’000,00
2	Quantity the ported numbers that can store into NP CDB after first system installation, not less than	5’000’000,00
3	The time required for monthly procedural operations, not more than	22 min.
4	Duration of treatment backup software and system configuration settings on the resources of internal storage, not more than	10 min.
5	The time required for full recovery system software from a backup with verification and testing functionality, not more than	60 min.
6	The time interval that is necessary to stop the service to return to an older version of the system software, not more than	10 min.
7	The interval of time that is necessary to stop	10 min.

	the service to extend the system hardware, not more than	
8	Update period (sync) Telcos' local databases (LDB) with the depositary NP CDB, provided at least 2 times a day	adjusted multiple of 60 min.
9	Period full backup of the NP CDB to backup storage, not less than	2 times per day
10	Storage period and availability of archived data on ported numbers in the system, not less than	5 years

2.7. The parameters of reliability of the system

No.	The parameters of reliability of the system	Value
1	Annual availability (uptime) NP CDB, not less than	99,9%
2	Annual availability (uptime) directory services system, not less than	99,0%
3	Annual availability (uptime) web-service of registration and processing of number portability applications, not less than	99,0%
4	Annual availability (uptime) the processing of number portability applications, not less than	99,9%
5	Annual availability (readiness index) of the DNS / ENUM / EPP, not less than	99,9%
6	Annual availability (readiness index) of the logging system, not less than	99,9%
7	RTT of the sequence of packets from the start of the TCP connection to its end, during access session to the PN CDN or FTPS, for at least 95% of the queries, not more than	1500 ms
8	RTT of the sequence of packets from the start of the UDP connection to its end, during access session to the PN CDN or FTPS, for at least 95% of the queries, not more than	500 ms