Proc. of the Second Intl. Conf. on Advances In Computing, Communication and Information Technology- CCIT 2014.

ISBN: 978-1-63248-051-4 doi: 10.15224/ 978-1-63248-051-4-22

# A Migration Decision for Users and Services Towards and Within the IMS

Sven Pärand

***Abstract*— Making the decision to migrate a user or service from a legacy network to a next generation network (NGN) requires thorough analysis. Despite the will and a clear necessity of telecom operators and service providers (SP) worldwide, many are still struggling with the migration process even after nearly five years and this can be attributed largely to the mentioned analysis aspect. New service delivery platforms (SDP) have necessitated the need to modernize or in some cases rebuild completely new operations support systems/business support systems (OSS/BSS). Mistakes have also been made in choosing an appropriate strategy for migration due to miscalculation in several key areas prior to migrating. Based on a task of moving users and services from legacy networks to IP multimedia subsystem (IMS) as well as inside the IMS, the current paper addresses the issue of making a solid migration decision, based on facts and proper analysis, concentrating mainly on the technical side of it. A high level migration process is presented to give an understanding of what a complete migration task entails. This is followed by a series of more detailed descriptions of specific steps and their sub-steps that contain key questions and issues that need addressing. The aim of this paper is to produce a generic guide or protocol for SPs and telecom operators to follow when making a migration decision.**

***Keywords*— *analysis, IMS, migration process, migration phases, NGN.***

## I. Introduction

The decision to migrate a user or service to or within a next generation network (NGN) [1] service delivery platform (SDP) should be based on detailed analysis. This means that every conceivable issue of the migration process must be broken down into smaller sub-processes and looked at from different angles to identify possible sources for failures during the actual migration itself. This paper makes a distinction between the overall migration process and the actual migration of users and services, the latter being a sub-step of the former.

As both short- and long term problems may arise in the migration process due to poor analysis and the fact that telecom operators and service providers (SPs) worldwide are still struggling with this matter, the current article is focused on two main goals. Firstly, to elaborate on the migration process and make a distinction between the, already mentioned, complete process and one of its sub-steps which is migrating concrete users or services.

Sven Pärand
Tallinn University of Technology
Estonia

A four step process is described in the paper. The aim of this paper is also to further specify the phases mentioned in the initial migration process with the ultimate goal of essentially creating a roadmap, in the form of flowcharts, for operators and service providers to follow while doing the analysis for migration. All of the issues raised are based on the notion that the SDP of choice for NGN is IP multimedia subsystem (IMS) [2]. Since the migration process can occur from legacy networks to IMS and also within the IMS, the latter option is disserted as well. A complete list of matters that need attention is, however, nearly impossible to create as this is highly dependent on the specific SP or operator.

For reaching the aims of the paper, the second and fourth step of the suggested process are presented in more detail. The first and third steps are omitted from the detailed description as the first phase, the pre-analysis, has already been considered in earlier literature. The third phase, the actual migrating of users and services, consists simply of acting upon the results achieved during analysis, i.e. computers running pre-determined scripts or humans following certain procedures to migrate the selected users or services. In addition, the introduced process takes into consideration the actions that need to be performed after the actual migration has taken place and which are not emphasized enough – the verification of results and monitoring for possible fault management.

The structure of this paper is as follows: the general four step migration process is described in Section II. This is followed by a discussion of all of the phases of the process in more detail: Section III sees the analysis phase being emphasized and Section IV concentrates on the activities after the migration has taken place, i.e. on the fourth phase of the suggested process. Section V concludes the paper.

## II. The Migration Process

The process a telecom operator or service provider has to pass through, to migrate its users and services to an NGN platform, can ultimately be defined. Naturally, this collection of phases cannot be standardized, as each company is different in a vast number of aspects, and nor should it be - there are only ideas and proposed solutions to make the transition to NGN as smooth and seamless as possible. The current section of this paper describes one possible general view of the mentioned process which will lay the foundation for successive sections where the presented flow chart will be further disentangled.

Fig. 1 illustrates a generalized four step process for migration. Before expanding on these phases in more detail, again, it must be emphasized that the focus of this paper is

Proc. of the Second Intl. Conf. on Advances In Computing, Communication and Information Technology- CCIT 2014.

ISBN: 978-1-63248-051-4 doi: 10.15224/ 978-1-63248-051-4-22

mainly on the second and fourth phase. The reason for this being the fact that the migration process is ongoing for most telecom companies worldwide, so the pre-analysis phase has already been passed through and needs no further elaborated discussion while the migration itself in the third phase is a trivial set of actions based on the analysis phase.

The first pre-analysis phase is where the operator or SP recognizes the need to migrate. This is usually caused by signals coming from the market or due to declining revenue and profit numbers. Whatever the reason, a clear shift in the business model of the company is realized and the second phase may be entered.

The analysis phase is the most important one since this is where the actual success or failure of the migration will be defined. Poor analysis may cause hard to fix or unrepairable damage in later phases. The different types of analysis done in this phase has been described and analyzed in [3].


Figure 1. A general view of the migration process to NGN.

The third phase is where the actual migration takes place. This phase is a direct consequence of the analysis phase and as mentioned depends on its thoroughness. The next generation service delivery platform is set up here, tested and eventually users and services will be transferred to it. It is imperative that throughout this stage the negative effects on customers should be as minimal as possible. This means the quality of service (QoS) must remain, at minimum, on the pre-migration level and the transition itself should be as seamless as possible.

The final phase in the migration chain is called post-migration processes. This is when the work done thus far has to be assessed and if need be, changes made. Also, constant quality measurement systems have to be put in place for proactive fault management and further QoS enhancement.

# III. The Analysis Phase

The activities undertaken in the analysis phase are essential and critical in the sense that any changes that need to be done after the completion of this phase can be attributed to poor analysis and considered highly resource encompassing.

Fig. 2 depicts, on a large scale, the different aspects that need attention in the analysis phase. Let it be noted that the figure is simplified and only the key factors are brought forth, in accordance with the initial aim of this paper.

The analysis can be divided into technical and non-technical. The latter part will not be elaborated on in detail here since the scope of this paper is more technical. Still, to mention a few keywords on the non-technical side – these would be resources and strategies. It is clear that any effort made by a service provider or telecom operator requires resources, both financial and non-financial (e.g. manpower, knowledge, cooperation with other companies). The relevant implementation choices for migration are described in more detail in [4].

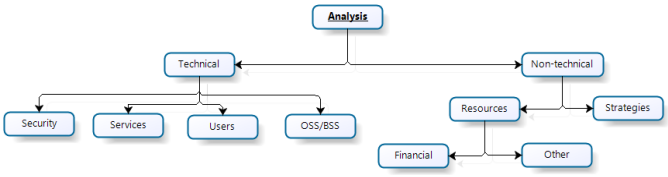


Figure 2. Top level overview of the analysis phase.

The technical side of the analysis is broken up into the following sub-steps: security, services, users and operating support system/business support system (OSS/BSS). Although the central idea of any NGN is to provide innovative and quality services to users, this cannot be done without appropriate security measures and functional supporting systems. Hence the mentioned items should be considered during the analysis. The following sections will describe all of the previously mentioned sub-steps in more detail.

## A. *Security*

Security in any system or network is a complicated matter that needs thorough consideration. Stemming from this and from the aim of the paper, the current article will not be able to describe an all-encompassing guide to analyzing all the possible security issues in IMS. A broad-based discussion on this topic has been published in [5], where threats to IMS implementations are examined. This paper will, instead, list the key factors that should be considered before migration which will in turn give hints to further research if and when the SP or operator deems it necessary.

The main considerations for a service provider regarding security can be classified into the following areas:

1) authentication and authorization for users and services;
2) access control for users and services;
3) information integrity and confidentiality;
4) use of proper communication protocols;
5) keeping track of activities in logs in a secure manner.

Based on the listed principles, Fig. 3 illustrates the analysis involved in the sub-steps of the security step.

Before addressing the actual IMS specific security matters in the analysis flow, the service providers' or operators' general constraints and concepts must be studied. These might for example include basic demands to areas such as outside access to company internal IP networks or support for specific protocols. The passing of this step in the analysis process lays the foundation for further, more detailed, security related nuances.

The following step, IMS specific concepts, can be divided into two major categories: IMS security services and operational security. The former is expanded upon in detail in [6] where a layered IMS security model is defined and the dependency of IMS security on the operators' general preferences is emphasized. Hence, in this step the analysis should mainly focus on clarifying the mentioned security

Proc. of the Second Intl. Conf. on Advances In Computing, Communication and Information Technology- CCIT 2014.

ISBN: 978-1-63248-051-4 doi: 10.15224/ 978-1-63248-051-4-22

model and choosing the suitable authentication method. In addition, since IMS is a network capable of cooperation with other networks, network domain security (NDS) will also have to be addressed. NDS comes into play when the users' first point of contact, the proxy-call session control function (P-CSCF), is located in the visited network.

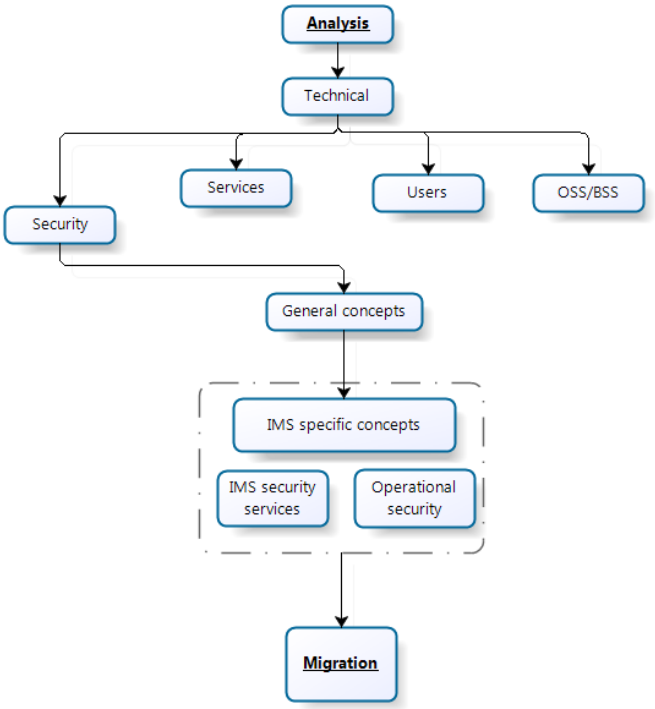


Figure 3. Analysis for security concepts.

As the IMS security services sub-step concentrates on major security aspects that will remain permanent after these have been decided, the operational security step might not be so static. The analysis here focuses on keywords such as P-CSCF discovery, user equipment (UE) registration, session initialization and termination, protection against different types of attacks and security management. As mentioned, some of these principles may change over time as for example attacks against the SPs or operators' network may become more evolved in nature.

The marked security management aspect is noteworthy and parallels may be drawn with any other system which, after initial startup, needs management. Security procedures and rules are no exception. This topic is dissected in [7] where it is concluded that the operational security of any NGN needs to have a strong security compliance program with the, not only support, but involvement of senior management. The security step analysis will eventually flow into the migration phase.

## B. *Services and Users*

The reason services and user analysis has been collocated under a single paragraph lies in their near identical analysis flow chart. The minor differences will be mentioned separately in the following description.

Figure 4 illustrates that the analysis starts with the notion of whether the user or service is IMS internal or external. In the external case, it is suggested that these will be migrated from legacy networks such as the PSTN. If this is the case, the matter of prudence should arise – is it worth wile for the operator or SP to start migrating the service or user? There is a possibility that the existing service based on PSTN is no longer supported in IMS or has changed to a large degree. A similar trail of thought applies to users. It might be more reasonable for the operator or SP to renounce the client as opposed to making substantial resource allocations to keep him or her. This is naturally only the case when the client absolutely has to be, for whatever reason, moved away from PSTN.

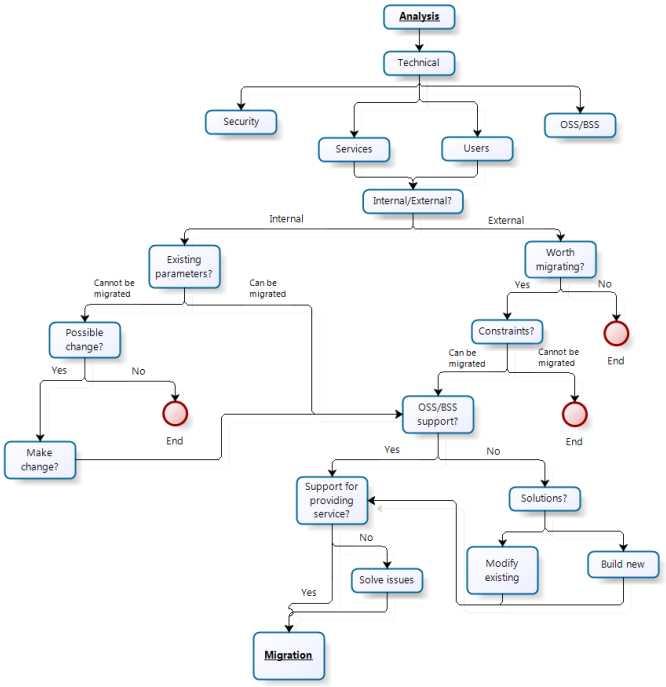


Figure 4. Analysis for migrating services and users.

In the event that the company, making the analysis, finds the user or service worthy of migration, all of the constraints attached to this user or service have to be determined. For example, these can be the issues regarding number portability or even missing copper wire or optical cable running to the customers' premises. Services usually have a myriad of nuances as well, which all have to be addressed separately.

Advancing further with the analysis in the external case, the support systems check has to be completed next. Neither the user nor any of the services can be moved without proper support from the OSS/BSS. If the analysis so far has resulted in a positive outcome as far as the migration decision is concerned, there are only two possible scenarios regarding the OSS/BSS: firstly, it might come to be that the existing support systems are already in a state of readiness to handle the new user or service and secondly, the opposite is true, in which case solutions are needed. The first scenario is however highly unlikely which means the operational support systems either need modifying or in the worst case scenario have to be built

Proc. of the Second Intl. Conf. on Advances In Computing, Communication and Information Technology- CCIT 2014.

ISBN: 978-1-63248-051-4 doi: 10.15224/ 978-1-63248-051-4-22

from the start. In any case, one or the other task will have to be completed to make the whole migration process eventually possible.

> However, the mistakes made could have been avoided and more importantly, can be avoided in the future if the SP or operator approaches the migration process analytically and in a detailed manner.

Lastly, upon completion of all of the previous steps, a final large scale readiness check has to be made. This might include the human resource and training, checking of all adjacent systems that do not fall under the OSS/BSS category, but also have to be in place for providing a service to a certain customer. The sub-step in question also entails looking at what happens after the service or user has been migrated - how or who takes care of the management, how are the client complaints handled etc. To be brief, this step of the analysis should mainly take a thorough look at the companies' internal processes and how these are equipped to handle operating in an NGN environment.

The left branch in Fig. 4 denotes the questions that should be addressed in case the migration task is IMS internal. This might happen when, for specific reasons depending on the SP or operator, the user or service must change application servers. Most of the logic here is similar to the situation where the user or service is external to the IMS. Still, there are differences in the initial part of the phase. Since the user or service is already in IMS, there is no need to consider if the migration is worth wile. Instead, it is of utmost importance to chalk down the existing parameters of the user or service with a high degree of precision. This mapping determines if and how the rest of the migration process will run its course.

When the details of the user or service reveal no obstacles for migration, the analysis can proceed straight to the supporting systems sub-step. However, upon discovering issues that prevent migration, changes have to be made. It is possible to modify either the users' or services' parameters or adjust the platform to house the migrated user or service. Only when it is clear that the modifications are feasible and possible in reality, can the analysis proceed again to the supporting systems sub-step.

## C. *OSS/BSS*

Similar to the security analysis, this paper will not be able to provide an all-encompassing description of every possible issue worth mentioning. Still, major components in the OSS/BSS analysis chain are highlighted based on Fig. 5.

Firstly, let it be mentioned that the support systems analysis is centered on two main notions: the central customer relationship management (CRM) and the task management, which are the backbone of the whole supporting realm. To differentiate the two, the CRM is considered to be the main tool for everyday use by the SP or operator and acts as an interface between a human being and the technical systems while the task management is essentially a system or a collection of systems which works in the background and either interprets the human input and acts accordingly or gathers data and translates it to a human readable form.

The product/services database is regarded as a collection of services descriptions and it should not be forgotten during the analysis. This threat exists as it is often not considered a part of the actual value chain, meaning it does not make real money. However, these descriptions are used whenever a service is initially built for a customer and also when a need arises to further develop the existing service in which case a solid start point, in the form of a detailed description, is in order. Hence, all the metadata about any given service must be considered carefully and saved in a corresponding data table. The main input for this database comes from the CRM.

The assurance sub-step analysis should focus on how the customer can approach the operator or service provider in case of need and how that request is processed. Different service levels have to be described and the corresponding tasks confirmed. An example first level point of contact for the customer may be a basic helpdesk, the second, a low level specialist and so on. As part of this analysis branch the interconnections of all of these levels must be described in parallel with specifying the systems and tools that are to be used for the management of the customer request. The flow should terminate with feedback. Its method and destinations are to be specified. As a default solution, both the client and the company providing the service need to know that the issue has been resolved. However, this may not always be the case.

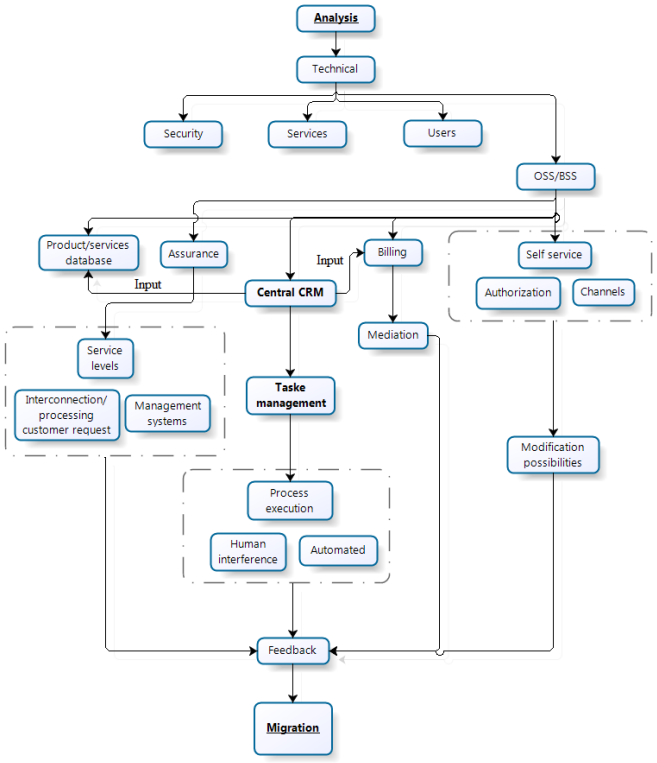


Figure 5. The OSS/BSS analysis flow.

As mentioned, the task management is responsible for performing a bulk of the concrete assignments in the

Proc. of the Second Intl. Conf. on Advances In Computing, Communication and Information Technology- CCIT 2014.

ISBN: 978-1-63248-051-4 doi: 10.15224/ 978-1-63248-051-4-22

OSS/BSS, ranging from provisioning new users to changing the configuration in a specific customer premises equipment (CPE). The main focus of analysis is directed towards elaborating the courses of action, i.e. how the process is executed, taken by the technical systems in achieving the end goal. This applies also in the case where human intervention in necessary. The last part of the chain considers, similarly to assurance, the issues of feedback.

The analysis process in the billing branch should focus on the mediation layer. Mediation in this case is a generic term and stands for an entity which collects and processes call detail records (CDR) data from various applications and sends it to a predefined location. The processing task is critical as the service provider or operator would eventually like to have all the CDR information in a similar form, however the CDR form in the application output may be proprietary and therefore vary from the desired outcome. A feedback or monitoring sub-step should also be regulated in billing as there may arise a need to troubleshoot the matter. In fact, feedback here could be considered extremely important since the billing system is the basis for writing invoices to customers.

Any modern telecom operator or SP today should strive to make as little contact with their customers as possible regarding day-to-day operations. This is not to say that contact with customers is bad but that simple requests made by the clients do not always need the interference of human resources. The self-service analysis in Fig. 5 concentrates on a way for the clients to make changes in their services by themselves. There are two main issues here to consider: first, the matter of authorizing the users and second, the channels through which customers can make their requests. The latter may include for example a web page or an interactive voice response (IVR) system.

After the authorization and request channels have been chosen, the actual modification possibilities must be analyzed. Clearly, a client may not be permitted to delete user accounts but simpler tasks, such as activating call recording for instance, are conceivable. Again, the flow ends with feedback in order to assure the customer that the desired changes have really been successful.

## IV. Post-Migration Processes

The post-migration phase is the final step in the general process of migration, depicted in Fig. 1. This can be, on a high level, divided into three major categories – verification, monitoring and management. Verification in this stage is considered to be a check to see whether the end result of the whole migration process towards NGN is successful. It must be noted, however, that process verification, which should be done in the, earlier, analysis phase, will also have to entail a verification sub-step. This area has been studied in more detail in [8], [9] and [10] where the need for process verification, both theoretically and empirically, has been clearly highlighted and several approaches for verification have been brought forth. However, as mentioned, in the context of the current stage of migration only the final outcome will be verified.

Depending on the migration, verification can be divided even further based on the type of verification as seen from Fig. 6. For example, if the migration process from PSTN to IMS is completed manually, the end result, or a major part of it, may also be verified manually. If the migration process is done automatically, the final check is also usually done without human interference. The type then ultimately dictates the procedures that have to be in place. The procedures contain information about who verifies, what and when. Additionally, an important procedure is giving feedback about possible issues to earlier stages of the migration process. This entails information regarding who or what systems are informed about the migration process having ended.

Monitoring may have many tasks which need to be identified when starting that sub-step. Firstly, it can be viewed as a source of information for fault management and therefore for any possible pro-active action done by the SP or operator. Secondly, it can act as a verification tool simply by indicating increasing activity in the NGN which refers to a constant successful migration process, assuming the migration process is not only IMS internal. Thirdly, monitoring provides vital information for future network planning in the sense that for example congestion issues will become visible in real time and this information will help in future network scalability planning.

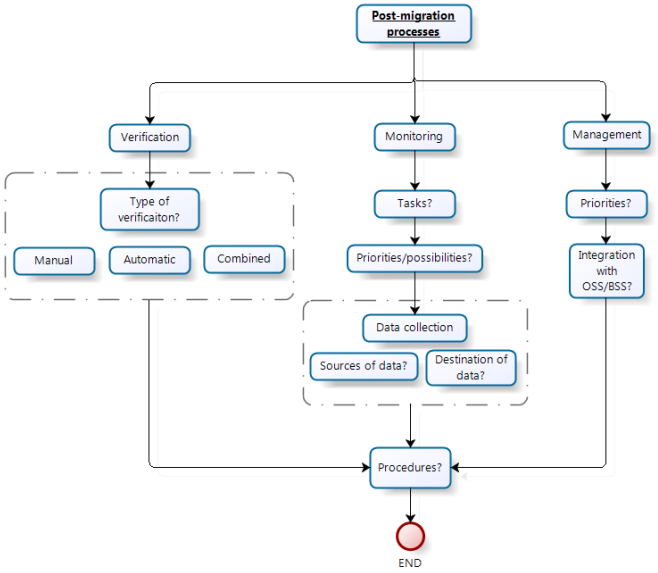


Figure 6. Post-migration processes flow.

Once the tasks of monitoring have been put in place, the SP or operator must consider the amount of nodes that can be monitored. Since a telecom company is usually working in a situation where recourses are limited, certain priorities have to be assigned to monitoring. In IMS the highest priorities should be assigned to the core nodes which make the operation of the NGN essentially possible. These are the call session control function (CSCF), home subscriber server (HSS), domain name system (DNS) and the border elements such as the session border controller (SBC). Naturally, provided there are ample amounts of resources, other nodes and systems can be added to this list.

Proc. of the Second Intl. Conf. on Advances In Computing, Communication and Information Technology- CCIT 2014.

ISBN: 978-1-63248-051-4 doi: 10.15224/ 978-1-63248-051-4-22

Next, the matter of data collection should be addressed, meaning the collected information from different sources will most likely have to be collected in a single point and processed to a human readable form. An example of this can be seen in Fig. 7 where the most important registration data of a CSCF is illustrated, i.e. accepted and rejected registrations and the response codes in the latter case.

The management branch in Fig. 6 comprises of initially describing priorities, just like in the case of monitoring. While it is clear that all the users and services will have to be managed to the full range of their properties, it is a question of priorities what will be done first, how and by whom. The management chain should ideally be integrated with the OSS/BSS, so this will have to be checked as well and any problems addressed. Finally, as with verification and monitoring, specific procedures will need to be put in place regarding the division of labor between both people and systems as well.

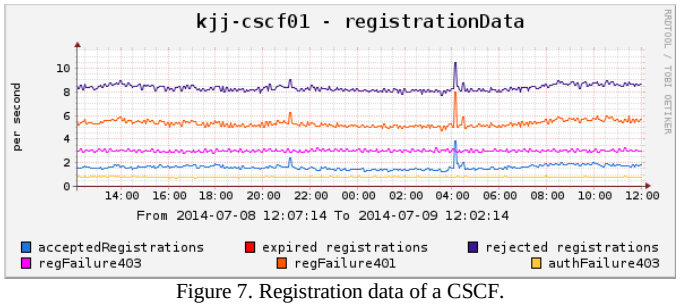

Figure 7. Registration data of a CSCF.

# V. Conclusion

Although service providers and telecom operators worldwide have been migrating users and services towards next generation networks for nearly five years they are still struggling with the process. This can be attributed to poor initial planning and analysis which has led some companies to a point where they need to start the process all over again.

However, the mistakes made could have been avoided and more importantly, can be avoided in the future if the SP or operator approaches the migration process analytically and in a detailed manner. The complete migration process can essentially be broken down into smaller phases, each one containing a collection of notions that need to be addressed and analyzed thoroughly. Clearly, a complete general list of problems can never be identified as these are dependent on an individual SP or operator.

Looking at the migration process and its phases, proposed in the current paper, it is clear that the most important phase is the analysis phase. The core questions to address there from a technical perspective are security, users, services and OSS/BSS. Each one has a different level of complexity and volume but none can be discarded as being unimportant. An issue worth mentioning is the fact that the analysis can not only be contained in the realm of legacy networks vs NGN, but all of the adjacent systems must be roped in as well. A good example of this is the OSS/BSS which does not offer a service to the customer per se but is still a crucial link in the complete chain of migration.

Emphasis must also be put into the actions which take place after the actual migration process has been completed. The results have to be verified, monitored for possible troubleshooting and finally, the users and services in NGN need management. All of the lastly mentioned keywords, if thought through and implemented properly, can help make the life of the SP or operator much easier and help keep client loyalty.

## Acknowledgment

The author would like to recognize Elion Enterprises Ltd. in general for its supporting and enthusiastic attitude during the writing of this article and also its many experts for their insights and comments on several key aspects of this paper.

## References

[1] *Series Y: Global Information Infrastructure, Internet Protocol Aspects and Next-Generation Networks*, ITU-T Recommendation Y.2001, 2004.

[2] G. Camarillo, M. A. Garcia-Martin, *The 3G IP Multimedia Subsystem: merging the Internet and the cellular worlds*, 3rd edition. Chichester, West Sussex, United Kingdom, 2008, pp. 25-48.

[3] Sven Pärand, "Migration towards NGN: common applied strategies," *International Journal of Computer and Communication Engineering*, vol. 2, no. 5, pp. 584-589, Sept. 2013.

[4] S. A. White, M. M. Clougherty, "PSTN migration using IMS," *Bell Labs Technical Journal*, vol. 13, Issue 1, pp. 199-219, May 2008.

[5] E. E. Anderlind, D. W. Faucher, E. H. Grosse, D. N. Heer, A. R. McGee, D. P. Strand, R. J. Thornberry Jr, "IMS security," *Bell Labs Technical Journal*, vol. 11, Issue 1, pp. 37-58, May 2006.

[6] M.Poikselkä, G.Mayer, *The IMS: IP multimedia concepts and services*, 3rd edition. Chichester, West Sussex, United Kingdom, 2009, pp. 113-126.

[7] S. Jacobs, *Security management of next generation telecommunications networks and services*, Hoboken, New Jersey, 2014, pp. 277-309.

[8] S. Patig, M. Stolz, "A pattern-based approach for the verification of business process descriptions," *Information and Software Technology*, vol. 55, Issue 1, pp. 58-87, Jan. 2013.

[9] M. Kaner, P. Soffer, "Complementing Business Process Verification by Validity Analysis: A Theoretical and Empirical Evaluation," *Journal of Database Management*, vol. 22, Issue 3, pp. 1-23, Jul. 2011.

[10] Nien-Lin Hsueh, Wen-Hsiang Shen, Zhi-Wei Yang, Don-Lin Yang, "Applying UML and software simulation for process definition, verification, and validation," *Information and Software Technology*, vol. 50, Issue 9-10, pp. 897-911, Aug. 2008.

**Sven Pärand** became a member of IEEE in 2012. He was born in Tallinn, Estonia, in 1982 and received his diploma in 2004 and M.Sc. with honors in 2006 in telecommunications from Tallinn University of Technology. He is currently a Ph.D. student at the same university.

From 2005 to 2012 he worked under the Ministry of Internal Affairs in Estonia. His main areas of responsibility were the introduction and development of private mobile radio and invulnerable phone systems. He is currently working at Elion Enterprises Ltd., part of TeliaSonera Group, in Estonia and is involved in research and development of applications for IP Multimedia Subsystem.