NASS-IMS bundled Authentication Study through Core Network Concepts

Giorgos Kostopoulos
Electrical and Computer Engineering Department
University of Patras
26500 RIO, PATRA, GREECE
Tel: +30 2610 997323
e-mail: gkostop@ece.upatras.gr

Odysseas Koufopavlou
Electrical and Computer Engineering Department
University of Patras
26500 RIO, PATRA, GREECE
Tel: +30 2610 996444
e-mail: odysseas@ece.upatras.gr

ABSTRACT
Emerging broadband access technologies are enabling the introduction of IP services to an increasing number of users. The market forecasts suggest that a new class of network providers will deploy public wireless or not networks based on these new technologies. In order to offer uninterrupted IP service combined with ubiquitous seamless mobility, these multi-provider networks need to be integrated with each other. As the latest descendant of such networks, the IP Multimedia Subsystem (IMS) has been envisaged to build up the extra functionality required to bridge such functionality gaps, hence accelerate services harmonisation in the context of mixed technology networks. Based on IMS architectural perception as well on ETSI TISPAN architecture, this article presents a complementary study of NASS-IMS bundled authentication on a core network communication concept. Finally, it concludes by focusing on its performance assessment through comparisons to different core network architectures and density of users.

Keywords
TISPAN, IP Multimedia Subsystem, NASS-IMS Authentication, SIP.

1. INTRODUCTION
The IP Multimedia Subsystem (IMS) standard defines a generic architecture for offering Voice over IP (VoIP) and multimedia services. It is an internationally recognized standard, specified by the Third Generation Partnership Project (3GPP/3GPP2) and embraced by other standards bodies including ETSI/TISPAN. The standard supports multiple access types including GSM, WCDMA, CDMA2000, wireline broadband access and WLAN. Users today welcome communication services that help them express their emotions and have fun, but also fulfil their practical needs - all in a style of communication they are used to. New IMS-based multimedia services have a key role to play in meeting users' expectations of more personal communication that brings them closer together, by making interaction as close as possible to a face-to-face experience.

The NASS is an access-level subsystem and provides registration at access level and initialization of user equipment for accessing to the TISPAN services. The NASS further provides network level identification and/or authentication, manages the IP address space of an access network connected thereto and authenticates access sessions. Network attachment through the NASS is based on implicit or explicit (user) subscriber identity and authentication credentials stored in the NASS. Thus, it is obvious that the NASS deals with some kind of access level authentication. The (core) IMS supports the provision of SIP-based multimedia services to subscribers or respective user equipments, wherein SIP stands for a session initiation protocol which is known to a skilled person. For this purpose, the IMS also has to deal with some kind of subscriber authentication. Accordingly, the two subsystems, i.e. the network attachment subsystem NASS and the IP multimedia subsystem IMS, normally perform separate authentication procedures for end users, i.e. subscribers.

Mobimedia'07, Month 8, 2007, Nafpaktos, Aitolokarnania, Greece

ACKNOWLEDGEMENT: This work is funded by VITAL IST Research Project. Contract Number: IST-2005-034284.

The solution to this situation is provided by NASS-IMS bundled Authentication [3, 4] schema. In this article a further study in this schema is presented using SIP signalling procedures as the mean to perform the study.

The rest of the article is organised as follows. In Section 2 are presented briefly the TISPAN, IMS and NASS architectures while in Section 3 is presented the overall procedure of NASS-IMS bundled Authentication. In Section 4 the experimental topologies are presented and in section 5 appear the methodologies we followed and the experimental results. The exploitation of the experimental results is given in section 6 while conclusions and future work are briefly presented in Section 7.

2. TISPAN-NASS-IMS
In this section we will present succinctly the Standards that the specific work resides in. The presentation sequence of the correspondent components will take place from wider architectural component to more specific. First of all the overall TISPAN architecture will be presented. The main functional top level components of TISPAN architecture will be presented. After that the IMS core architecture including ETSI TISPAN components will briefly explained. Finally, it will be given a description of the NASS functional entity of TISPAN. Specifically, the main components of NASS, especially these are getting involved in the present research work, will be described.

2.1 TISPAN
TISPAN Release 1 was published in December 2005. The Release 1 architecture is based upon the concept of cooperating subsystems sharing common components. This subsystem-oriented architecture enables the addition of new subsystems over

the time to cover new demands and service classes. The architecture ensures that the network resources, applications, and user equipment are common to all subsystems and therefore ensure user, terminal and service mobility to the fullest extent possible, including across administrative boundaries. One of the key subsystems is based upon the 3GPP IP Multimedia Subsystem (IMS) Release 6 and 3GPP2 Revision A architectures. In Figure 1 the overall architecture of TISPAN is presented.

The service layer comprises of the following elements:

- the core IP Multimedia Subsystem (IMS);
- the PSTN/ISDN Emulation Subsystem (PES);
- other multimedia subsystems (e.g. streaming subsystem, content broadcasting subsystem etc.) and applications;
- common components (i.e. used by several subsystems) such as those required for accessing applications, charging functions, user profile management, security management, routing data bases (e.g. ENUM) [1], etc.

More can be found in [2].

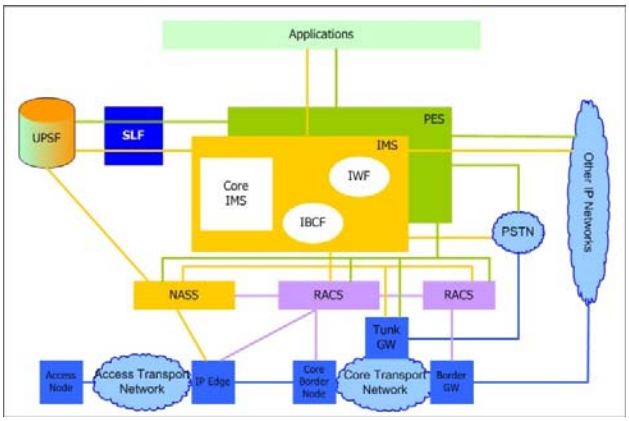

Figure 1. Overall TISPAN Architecture

2.2 IMS

The 3GPP IP Multimedia Subsystem (IMS) is rapidly becoming the de facto standard for real-time multimedia communications services. Although the IMS was originally specified for 3G mobile networks, it also provides excellent service deployment architecture for any fixed or wireless network, and all IP-based networks such as WiFi, corporate enterprise LANs, and the public Internet. IMS standards define open interfaces for session management, access control, mobility management, service control, and billing. This allows the network provider to offer a managed SIP network, with all the carrier-grade attributes of the switched circuit network, but at a lower cost and with increased flexibility. In addition, the use of SIP [6] as a common signalling protocol allows independent software developers to leverage a broad range of third party application servers, media servers, and SIP-enabled end user devices to create next generation services.

The IMS architecture is evolving across multiple 3GPP releases. For example, Release 6 includes Wireless LAN access mechanisms; and Release 7 includes broadband/wireline access capabilities. The Figure 2 shows the 3GPP IMS architecture including ETSI TISPAN functionality in order to highlight the coordinated compatibility between the efforts. More can be found in [7],[10],[11].

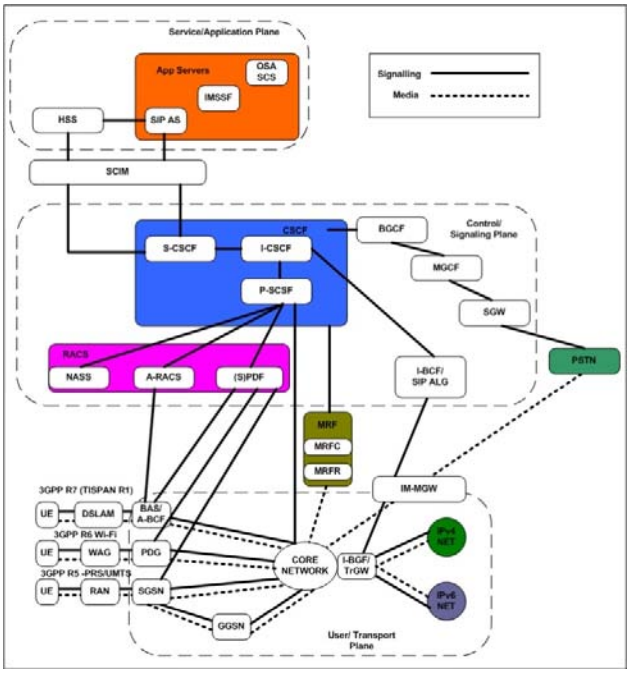

Figure 2: The 3GPP IMS Architecture including ETSI TISPAN components

2.3 NASS Security Entities

The Network Attachment Subsystem (NASS) comprises of the following security related functional entities that are relevant for Access Domain Security*:*

Customer Network Gateway (CNG), this entity requests access from the network.

The Access Management Function (AMG), this function forwards requests to the User Access Authorization Function (UAAF) to authenticate the user, authorize or deny the network access and retrieve user-specific access configuration parameters.

The User Access Authorization Function (UAFF) performs user authentication, as well as authorization checking based on user profiles for network access. For each user, UAAF retrieves authentication data and access authorization information from the user network profile contained in the Profile Data Base Function (PDBF).

The Profile Database Function (PDBF) is the functional entity that contains user authentication data (e.g. user identity, list of authentication methods, authentication keys, etc.) and information related to the required network access configuration.

The Connectivity Session Location and Repository Function (CLF). The Connectivity Session Location and Repository Function (CLF) registers the association between the IP address allocated to the UE and related network location information provided by the NACF, i.e.: access transport equipment characteristics, line identifier (Logical Access ID), IP Edge identity, etc. The CLF registers the association between network location information received from the NACF and geographical location information. The CLF may also store the identity of the user / UE to which the IP address has been allocated (information received from the UAAF), as well as the user network QoS profile and user preferences regarding the privacy of location information. In case the CLF does not store the identity/profile of the user/UE, the CLF shall be able to retrieve this information from the UAAF. The CLF responds to location queries from service control subsystems and applications. In the following

figure is presented the NASS architecture containing the pre-mentioned functional entities.

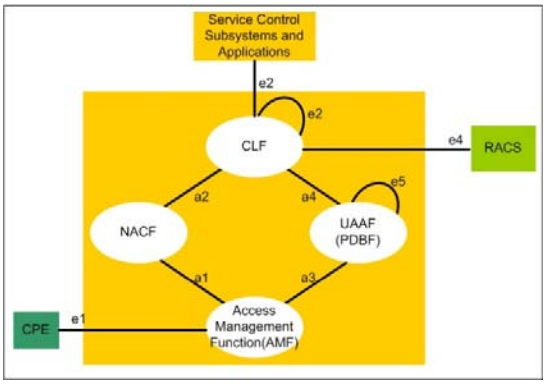

Figure 3: NASS Architecture

Further analysis of NASS can be found in [5].

3. NASS-IMS BUNDLED AUTHENTICATION

In this section the NASS-IMS bundled authentication is briefly presented. SIP signalling is the primary method for user registration and session control in the IMS architecture. The outline model for authentication is presented in the following picture. The main components of the authentication pattern are: the key manager, the claimant (user), the verifier and finally the Verifier Proxy. The result of authentication is accessed by IMS.

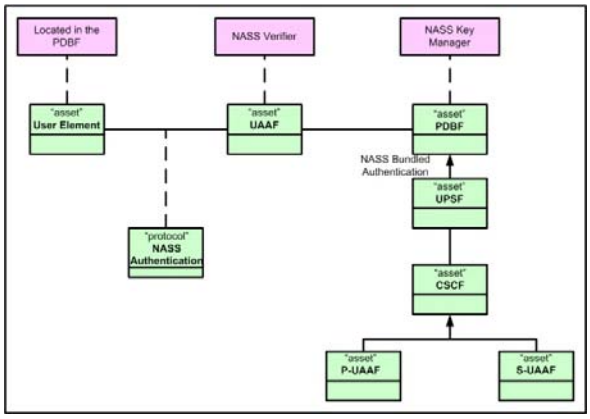

Figure 4: Authentication Pattern

The assets that are involved in IMS-NASS bundled authentication are:

Connectivity Session Location and Repository Function (CLF).

Call Session Control Function (CSCF):

- Interrogating - Call Session Control Function (I-CSCF).
- Proxy - Call Session Control Function (P-CSCF).
- Serving - Call Session Control Function (S-CSCF).

User Equipment (UE).

User Profile Server Function (UPSF).

Authentication Protocols:

- NASS authentication - Between UE and CLF.
- NASS-IMS bundled -Between UE, CLF, CSCF, and UPSF.

In the following diagram is described how clients authenticate to NASS and simultaneously also given service layer authentication using the NASS bundled authentication.

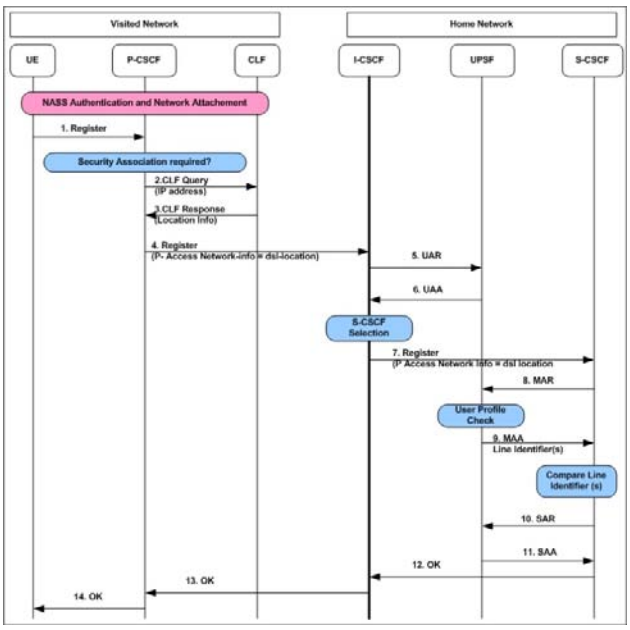

Figure 5: Flow Diagram for NASS-IMS Bundled Authentication

The full explanation of the above flow diagram is described in [4].

4. EXPERIMENTAL TOPOLOGIES

In this section it will be presented three different topologies and scenarios we chose in order to perform SIP signaling analysis and study their behavior. The criteria we chose the following topologies are complying with some of the fundamental aspects of NGN architectures [12].

Taking account the above we chose the three following scenarios that are mapping in “real world” network topologies as well as to the NASS-IMS Bundled authentication procedure. In the first scenario the Service Control Subsystem is provided by the visited NGN network. (Scenario 1 – Figure 6),

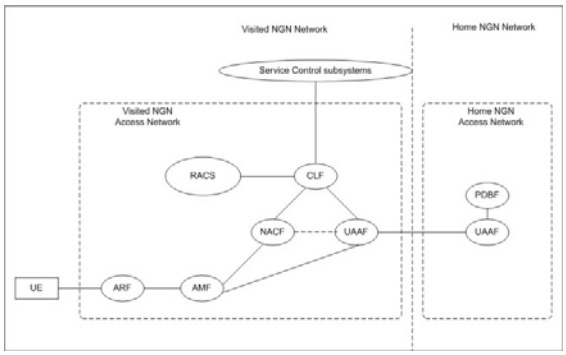

Figure 6: Service provided by Visited NGN

while in the second scenario the Service Control Subsystem is provided by the home NGN network (Scenario 2 – Figure 7).

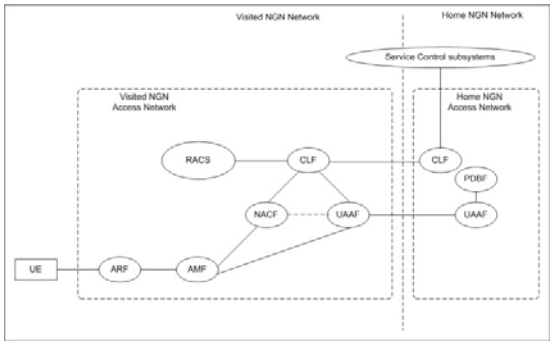

Figure 7: Service provided by Home NGN

Finally, in the third scenario the Service Control Subsystem is provided by the visited NGN network via Proxy CLF (Scenario 3 – Figure 8).

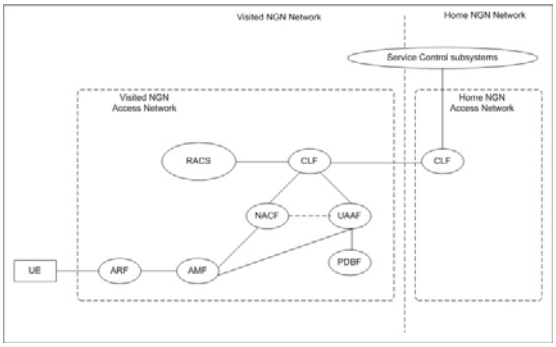

Figure 8: Service provided via Proxy

5. EXPERIMENTAL RESULTS-METHODOLOGIES

The testing we performed was based in the pre-mentioned scenarios. We used these scenarios in order to test the behavior of the evolving components during NASS-IMS Bundled Authentication. The reason we used these scenarios and not something else is that we wanted to test the procedure using scenarios that happen often in "real-world"; many users will try to use the service.

We emulated the SIP exchange messages using SIPp [10] tool and all the measurements have been made using SIPp. This tool accepts as input xml files. So, we created xml files that are fully compliant with the desirable call flows with real parameters. SIPp taking as input our xml files was reproducing the scenario. All the scenarios and measurements took place after the network attachment procedure. During this procedure we defined a priori the GPRS attach, PDP Context Establishment and P-CSCF Discovery functions. The algorithm mode we used for Authentication was AKAv1-MD5 as specified by 3GPP for IMS and was supported by SIP. The Operating System we used to run the tool was the Fedora Core 4. All the tests run on Intel Centrino Duo 1,83 GHz T2400 CPU.

We run tests and measured the response times, using SIPp for the following respectively for three scenarios and the following cases:

From UE to P-CSCF

The purpose of this request is to register the user's SIP URI [11] with an S-CSCF in the home network. This request is routed to P-CSCF because it is the only SIP server known to UE.

From P-CSCF to I-CSCF

In this case P-CSCF needs to be in the path for all mobile terminated requests for this user. To ensure this, P-CSCF adds itself to the Path header value for future requests. P-CSCF adds the P-Visited-Network-ID header with the contents of the identifier of P-CSCF network. This is the NASS location information.

From I-CSCF to S-CSCF

In this case I-CSCF does not modify the Path header and S-CSCF stores the contents of the Path header and uses the URI for routing mobile terminated requests.

Finally, it has to be noticed that all the measurements have been taken for a non-registered user.

It has to be mentioned that we were running the full call (UE → S-CSCF) and we measured the response time divided into three stages, one for each test case. We made 20 continuous calls in order to have quite satisfying number of samples. The calls were made one by one; after the completion of one full cycle we were starting the next. The results of the testing that was performed are overall presented in the following table. In the table are presented the minimum, maximum and average response time for each case for the three scenarios. Finally the total time per cycle is given for three scenarios.

Table 1: Overall Results for SIP calls response time

Test Case		**UE to P-CSCF**	**P-CSCF to I-CSCF**	**I-CSCF to CSCF**	**Total: UE to S-CSCF**
Scenario 1	Min. (ms)	22.7	278.82	96.24	397.76
	Max. (ms)	26.99	283.11	100.53	410.63
	Avg. (ms)	24.98	281,10	98.52	404.61
Scenario 2	*Min.* (ms)	32.56	442.42	235.69	710.69
	Max. (ms)	43.53	711.90	337.73	1093.17
	Avg. (ms)	37.93	539.39	289.95	867.26
Scenario 3	Min. (ms)	30.09	375.59	228.05	633.73
	Max. (ms)	34.38	505.66	330.54	870.58
	Avg. (ms)	32.37	421.38	280.97	734.72

Using the results from the measurement procedure we produced the following graphical representations in order to depict the behaviour of the system. In order to achieve better exploitation we represented separately the results for each stage of a full call. We created three charts for each stage including the results of the three scenarios: UE to P-CSCF, P-CSCF to I-CSCF and I-CSCF to S-CSCF respectively.

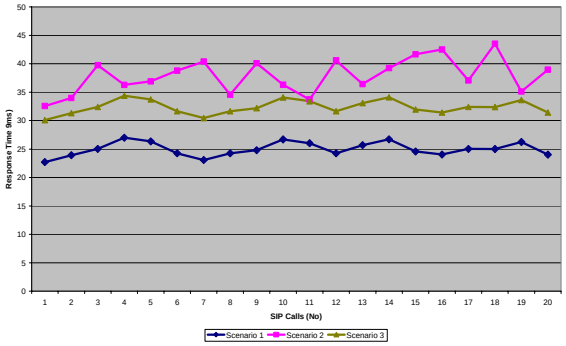

Figure 9: Graphical representation of response time for UE to P-CSCF for three scenarios

Respectively in the following figure the graphical representation of the measurements during the P-CSCF and I-CSCF SIP calls is presented.

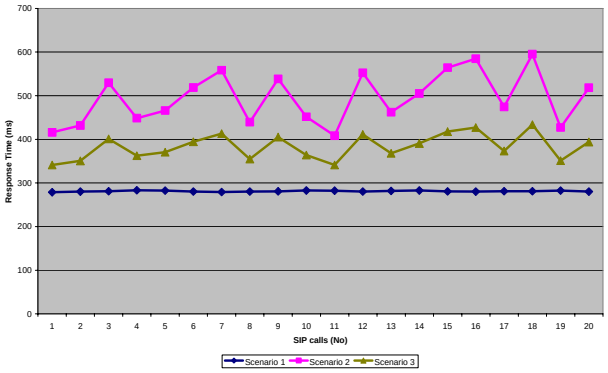

Figure 10: Graphical representation of response time for P-CSCF and I-CSCF SIP calls

Finally, in the next figure the graphical representation of the measurements during the I-CSCF and S-CSCF SIP calls is presented.

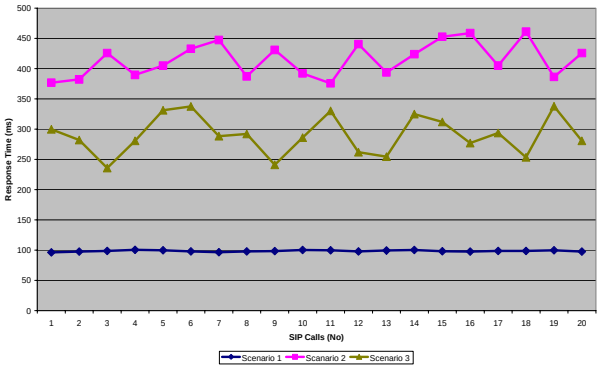

Figure 11: Graphical representation of response time for I-CSCF and S-CSCF SIP calls

The exploitation of these representations will be fully presented in the next section of the present article.

The next step in this study was to perform measurements in the case that multiple users were attempting to get services. For this case also we used the SIPp tool. The testing infrastructure was the same as in previous test. This time we run the tests only for the basic scenario of NASS-IMS bundled authentication that depicted in figure 6 of the present article. The concept here is to have simultaneously multiple users attempting to gain access control. We chose three different cases:

a) 30 SIP calls/sec for 20 seconds continuously (600 calls in 20 sec time period);

b) 10 SIP calls/sec for 20 seconds continuously (200 calls in 20 sec time period);

c) 5 SIP calls/sec for 20 seconds continuously (100 calls in 20 sec time period).

Also, in this test we had the opportunity to monitor the full call through three stages, UE to P-CSCF, P-CSCF to I-CSCF and I-CSCF to S-CSCF respectively. The overall results of this test are presented in the following table:

Table 2: Number of Successful/Total calls

Test Case	30 Calls/s for 20 sec	10 Calls/s for 20 sec	5 Calls/s for 20 sec
Successful Calls	117/600	98/200	83/100
UE to P-CSCF	539/600	188/200	97/100
P-CSCF to I-CSCF	132/539	107/188	87/97
I-CSCF to S-CSCF	117/132	98/107	83/87

The experimental results are graphically represented in the following charts. In the first chart is presented the percentage of the successful calls for three cases.

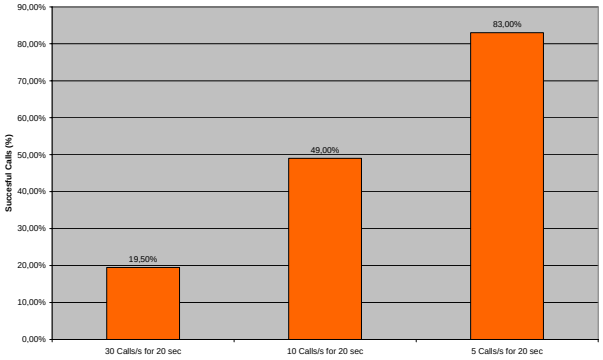

Figure 12: Percentage of the successful calls

In the next graph are presented the successful calls (%) per stage, UE to P-CSCF, P-CSCF to I-CSCF and I-CSCF to S-CSCF respectively.

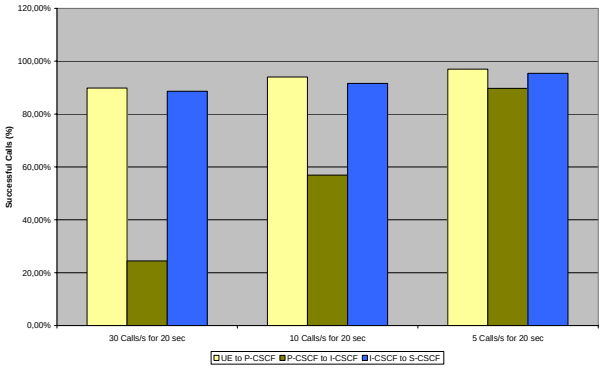

Figure 13: Successful calls (%) per stage

The further exploitation of the results will be presented in the following section of the article.

6. EXPLOITATION OF THE RESULTS

In this section it will be presented and analyzed the results of the experimental part. For better presentation purposes we will divide into two separate subsections the exploitation analysis. In the first subsection it will be analyzed the results arouse from the first experimental part (call by call for three topologies) whilst in the second subsection it will be analyzes the results from the second test case (simultaneously) users calls.

6.1 First Experimental Part

Through the results of the measurements performed for the three different scenarios came up the following results. We notice that the latest response time (total) occurs during scenario 2 (Service provided by home NGN) while the quickest response time occurs during scenario 1 (Service provided by Visited NGN. In scenario 3 the use of Proxy CLF we notice that improves the response time. So, if there could be a hypothetical categorization among the three scenarios into these that the Service is provided by Home NGN and those that the service is provided by Visited NGN we can compare the Scenario 2 and Scenario 3 response times and come up to the conclusion that the Proxy CLF improves the response time and consequently the QoS of this topology. On the other hand on the topology of Scenario 2 the need for better network management is something more than essential. Let's remind that the procedure took place with one call by call. What could be the result if multiple users were trying to get access? This will be exploited into the second part of this section. Another useful conclusion that came up through the experimental results is that we can take advantage from the case that the service is provided by the Visited NGN.

Through the step by step analysis that was performed we also noticed that the latest response time occurs during the P-CSCF to I-CSCF phase also in three scenarios. That major delay arises from two major factors through the NASS. One factor is the delay that comes up during the update of the P-CSCF header. The P-CSCF adds the P-Visited-Network-ID header with the contents of the identifier of P-CSCF network. The other reason is the CLF function that takes place again in the NASS. CLF function is very critical during the NASS-IMS bundled authentication since it performs some major functions such as: User IP registration, stores the identity of the user, stores the QoS of the user, etc. the point that comes up in this case is also the need for better management especially in during CLF function. This need is also proven especially in the second experimental part.

6.2 Second experimental part

In this part we tried to study the behavior of the topologies in case of multiple users, case that is very close to a business scenario. As mentioned in the methodologies section we used three different cases of multiple users. Looking at the chart of Figure 12 we notice that the percentage of the successful calls was very low when the number of users was getting bigger in the same time slot. Trying to explain this behavior we analyze further this behavior by splitting into three different stages the full call. Having a look at the chart in the Figure 13 we notice that in all the cases the bigger percentage of dropped calls arouse during the P-CSCF to I-CSCF phase. Especially in the case of the 30 calls/sec during 20 sec the dropped calls are mainly caused through the time out during P-CSCF to I-CSCF phase. The percentage of successful calls (19,5%) is very disappointing. Passing to the second case 10 calls/sec during 20 sec we notice that the situation of the missed calls is inclined to be regulated (49% successful calls) but it is also not a very good number. Similar with previous the stage that is responsible for the dropped calls is the P-CSCF to I-CSCF. Finally, in the case that the users per sec are less then we notice that we have a normal percentage of successful calls. As it was mentioned previous the reason of this subnormal behaviour is the CLF function.

7. CONCLUSIONS-FUTUE WORK

In this article a study in the NASS-IMS bundled authentication for three different network topologies was presented. IMS and ETSI TIPAN architectures were presented and was noticed their significance in the networked communication world. Three different topologies were chosen in order to apply the NASS-ISM bundled authentication procedure. The procedure took place through several experimental parts performing SIP signaling analysis and very useful conclusions came up. The results that came up will lead us in further research in management aspects in NGN. ETSI TISPAN through IMS is a huge research topic and a lot of effort is required in order to improve it and cover all the aspects that possibly affect the network access. Next step of this effort will be the improvement of the CLF management function in terms of timing, security and assurance of quality to the customer. The development of new innovative techniques and models during CLF functionality is the next target.

8. REFERENCES

[1] P. Faltstrom, M. Mealling, "The E.164 to Uniform Resource Identifiers (URI) Dynamic Delegation Discovery System (DDDS) Application (ENUM)", RFC 3761 (Standards Track), April 2004.

[2] ETSI ES 282 001, Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); NGN Functional Architecture Release 1.

[3] ETSI TS 187 003, Telecommunication and Internet converged Services and Protocols for Advanced Networking (TISPAN); NGN Security; Security Architecture.

[4] ETSI TR 187 002, Telecommunication and Internet converged Services and Protocols for Advanced Networking (TISPAN); TISPAN NGN Security (NGN_SEC); Threat and Risk Analysis.

[5] ETSI ES 282 004, Telecommunication and Internet converged Services and Protocols for Advanced Networking (TISPAN); Network Attachment Subsystem (NASS).

[6] J. Rosenberg, H. Schulzrinne, G. Camarillo, A. Johnston, J. Peterson, R. Sparks, M. Handley, E. Schooler, "SIP: Session Initiation Protocol", RFC 3261 (Standards Track), June 2002.

[7] 3GPP TS 23.228, 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; IP Multimedia Subsystem (IMS); Stage 2, (Release 7).

[8] http://sipp.sourceforge.net/index.html .

[9] T. Berners-Lee, R. Fielding, L. Masinter, "Uniform Resource Identifiers (URI): Generic Syntax", RFC 2396 (Standards Track), August 1998

[10] Th. Magedanz, F.C. de Gouveia (2006), "IMS – the IP Multimedia System as NGN Service Delivery Platform", Elektrotechnik & Informationstechnik, 123/7/8: 271-276.

[11] Muhammad Sher and Thomas Magedanz, "Secure Access to IP Multimedia Services Using Generic Bootstrapping Architecture (GBA) for 3G & Beyond Mobile Networks", Q2SWinet'06, pp 17-24.

[12] http://www.itu.int/ITU-T/studygroups/com13/ngn2004/working_definition.html