

Proposed solution for improving the reliability of HSS data by integrating a queue manager

Ngartabé KAG-TEUBE*, Yvan Paillard KALIA-SYA DODOAGNEN*, Samuel OUYA*, Kéba GUEYE*

*Laboratory LIRT, Higher Polytechnic School, University Cheikh Anta Diop of Dakar, Senegal

kagteubedaniel@gmail.com, vanyvan10@gmail.com, samuel.ouya@gmail.com, mamekeb@gmail.com

Abstract— The current trend is towards rich communications services (RCS). SCRs define a set of services that network operators can provide through the IMS architecture, including voice and video calls, instant messaging, and so on.

Indeed, the IMS is considered today as the base to provide the new services and to converge all the existing means of communication. The IMS has a central element called HSS. HSS is a database that stores user-specific data, access settings, service invocation rules, and billing data.

However, it is important that the authentication information exchange mechanisms based on the DIAMETER protocol are clear, since a malfunction can negatively impact the quality of service (QoS) and the profits of the operators.

Moreover, it should be noted that a lot of research work around VoLTE has been conducted in recent years with free software implementing the IMS core network, like SER platforms such as: OpenIMSCore and KAMAILIO.

Otherwise, various tests were carried out with the KAMAILIO platform coupled with the openIMSCore HSS to build an IMS core network.

During these tests, various observations are made on the analysis of the registration messages, following which two problems were identified:

- The HSS entity displays on its interface the "connected status" of the users, while the latter cannot connect;

- When a user who is logged out leaves his / her session, the HSS entity does not display on its interface that the user is disconnected.

Finally, this paper aims to highlight the dysfunction observed during registration message exchanges and to propose a solution to improve the reliability of the HSS data by integrating a queue manager. This handler will

interact between the I-CSCF, S-CSCF and HSS entities so that when transferring or downloading the user's profile, the HSS entity does not display that the user is logged in without having the confirmation the S-CSCF entity that its profile is stored in the location table (called location) to then trigger the sending of the "SIP 200 OK" notifying the user that it is registered.

Keywords— RCS, IMS, Convergence, HSS, SIP, DIAMETER, VoLTE, SIP, Kamailio.

I. INTRODUCTION

Mobility is an important aspect to consider in the service proposal, as users want simple, transparent, secure, portable and reliable communications services.

The convergence of communication services leads to an All-IP architecture, facilitating the development of services that combine both telecommunications and IT, offering a potential for a rich variety of communication to end-users.

However, the current trend is to go to rich communication platforms. Rich Communication Services (RCS) defines a set of services that network operators can provide using the IMS, including voice calls and video, instant messaging, individual and group chat, file transfer, presence and geolocation.

Thus, VoLTE consists of an implementation by the association of the EPS network for the transport of the flows and the IMS network for signaling processing [1] [2] [3] [4]. Indeed, the IMS is an architecture that makes it possible to converge all the existing means of communication. For the delivery of services, the IMS is based on the SIP multimedia logon protocol [5] [6].

In recent years, much of the research has been conducted around the IMS architecture. To do this, researchers rely on or develop free platforms implementing the core of the IMS network. This is the case of the OpenIMSCore project, and very recently the modules of KAMAILIO and also a free platform from the SIP Express Router. KAMAILIO is a modular and extensible SIP proxy [2] [5] [14].

In its architecture, IMS relies on the HSS entity to store user profiles and service profiles. The HSS contains information's that allows the user to be located but also to associate the service profiles. The malfunction of the HSS will

have a negative impact on the quality of service but also on the profits of the telecom operators. To locate a user, the HSS communicates with Call Session Control Function (CSCF) through the Diameter protocol.

In order to have a converged telecom network offering both high-speed mobile data and high-quality telephone services, we need an IMS network.

The IMS network defines the routing of telephone signaling, access to databases where the profile and the subscriber's secret are stored, as well as the specific processing of the voice.

IMS provides the entities that provide protocol conversion and the interconnection of fixed and mobile networks. The anchoring of signal and voice flows is done using the Single Radio Voice Call Continuity (SRVCC) mechanism [1] [2].

The HSS plays an important role in the indication of the Access Point Name (APN) and also provides access to the profile and security data of the mobile.

The HSS entity is a database that stores specific data to each user. The stored data includes user identities, access parameters, and rules for invoking application servers by the S-CSCF.

Moreover, online or offline charging is based on the DIAMETER protocol. DIAMETER is the exchange protocol between the key entities of the IMS network. Therefore, the mechanisms implemented in the exchanges must be reliable to ensure the reliability of the data stored or processed by the entities of the core of the IMS network [9] [10].

In this work, we have implemented a platform based on the Kamailio IMS modules and the HSS entity of the OpenIMSCore project to highlight the defects in the reliability of the HSS data following the non-reception of the confirmation message of the HSS S-CSCF entity. We have seen a malfunctioning of the platform we have put in place. The experiments carried out on this platform enabled us to identify the limitations in the operating mechanism of the DIAMETER protocol.

The objective of this work is to improve the operation of the HSS, which uses the DIAMETER protocol to exchange with the CSCF functions of the IMS.

We propose in this paper the introduction of a queue manager to help remove the dysfunction found during the tests performed.

The rest of the paper is structured as follows: Section 2 is devoted to the state of the art on the IMS, the DIAMETER protocol and the KAMAILIO IMS modules. In Section 3, we present the results and discussion the design of our solution and in Section 4, the conclusion.

II. STATE OF THE ART

It is proposed to build an IMS network core from the KAMAILIO platform. The idea proposed in this paper is to show the registration procedures in IMS by identifying the different messages or exchanges between the I-CSCF, S-CSCF and HSS entities. The procedures in IMS are based on exchanging SIP and DIAMETER messages. We will state the art of what exists as follows:

A. Presentation of the IMS

IP Multimedia Subsystem (IMS) is a layered architecture that provides integrated IP multimedia services. It is based on the Session Initialization Protocol (SIP) to support service session control functions. Originally, it is designed for 3G networks (by 3GPP) and is not related to access and transport techniques. The IMS is now the nucleus of Next Generation Network (NGN) [7] to provide multimedia services. In the IMS network, we can create a variety of applications by environment and service creation strategies. Figure 1 illustrates the architecture of the IMS network.

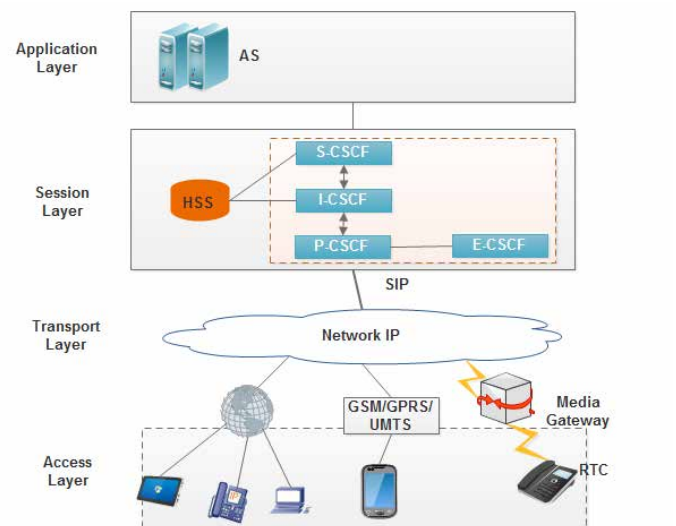


Figure 1. Layer architecture of the IMS

B. SIP Signalling

SIP (Session Initiation Protocol) is a signalling protocol defined by the Internet Engineering Task Force (IETF) for the establishment, release and modification of multimedia sessions. SIP is used in the IMS as signalling protocol for session control and service control. It thus replaces both the ISUP (ISDN User Part) and Intelligent Network Application Part (INAP) protocols of the telephony world by providing the multimedia capability [8]. SIP is the backbone of the IMS architecture. Its use implies that of the associated protocols, in particular SDP, for the description of the sessions, and RTP / RTCP, for the real-time transport (and control) of multimedia data streams.

At the IMS, SIP is used by the IMS network equipment (CSCF in particular) to control the call (establishment, modification, end) during any multimedia session. A session is established as soon as two or more participants exchange data. SIP can handle multicast, group or automatic calls.

In any type of network, there are always four types of signalling:

- Registration signalling: by it, a terminal registers in the network. It contains the procedures for downloading the profile and managing the location.

It is performed by the SIP registration procedure (SIP REGISTER).

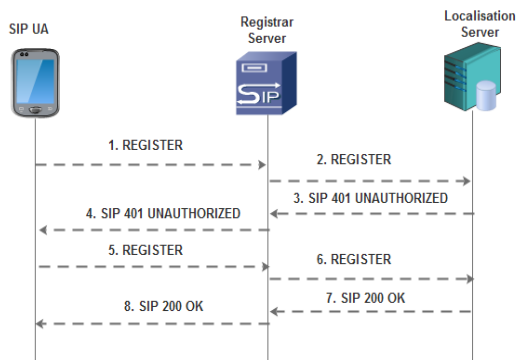


Figure 2. Registration procedure SIP REGISTER

- Call signalling : by it an end-to-end association is established between the end points wishing to communicate. This type of signalling is characterized by reference exchange. This is done in IMS through the session setup procedure (SIP INVITE).

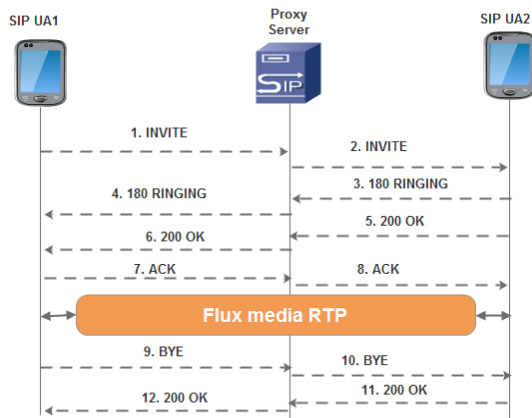


Figure 3. Setup procedure INVITE session

- Signalling connection: it is the assignment of a support service to a call. Step by step we will reserve resources in the network according to the QoS required for the service. In SIP, this signalling is done using the SDP headers that describe the traffic and the resources required. At the transport level, Resource Reservation Protocol (RSVP), DiffServ (Differentiated Services), are used to ensure quality of service in the IP network.
- Intelligence signalling: it makes it possible to do a substitutive treatment with respect to the normal call processing. In a similar way to intelligent networks of type RI (INAP) or CAMEL, the services are executed by the equivalent to the service platforms which are application servers (AS) [8].

C. DIAMETER protocol

DIAMETER is an advanced protocol that is generally regarded as a next-generation protocol in the IP Multimedia

Subsystem (IMS) architecture and LTE networks. It provides higher data rates and increased network throughput and provides of AAA services. Authentication, Authorization and Accounting (AAA) are core network functions used to track user activity and consumption of network resources [9] [10] [14].

A DIAMETER architecture is composed of different nodes called "DIAMETER Agents". Each node has a well-defined task. They form a so-called peer-to-peer network.

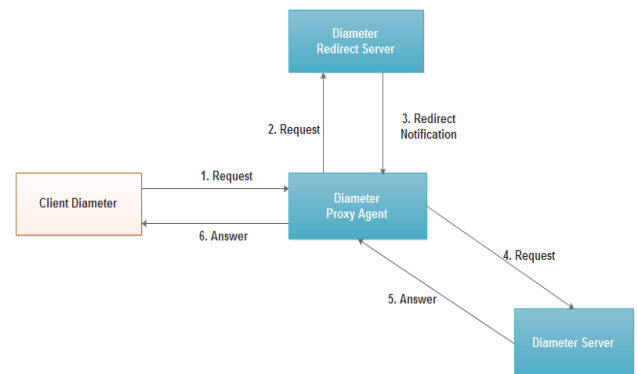


Figure 4. Basic DIAMETER protocol architecture

D. DIAMETER SIP Application Recording Diagram

DIAMETER SIP Application can be used in a SIP environment where an interface for an AAA infrastructure that requires authentication and authorization to use SIP resources. This application provides support for SIP user agents and proxies that implement and use HTTP Digest authentication, it is the authentication mechanism required by the SIP protocol.

Figure 5 below shows a general overview of the integration of the SIP architecture with the AAA architecture.

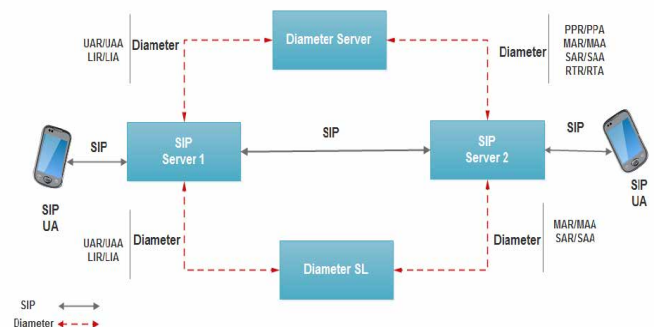


Figure 5. General architecture SIP DIAMETER Application

According to RFC 4740 [11], the proposed diagram for a user record is described as follows:

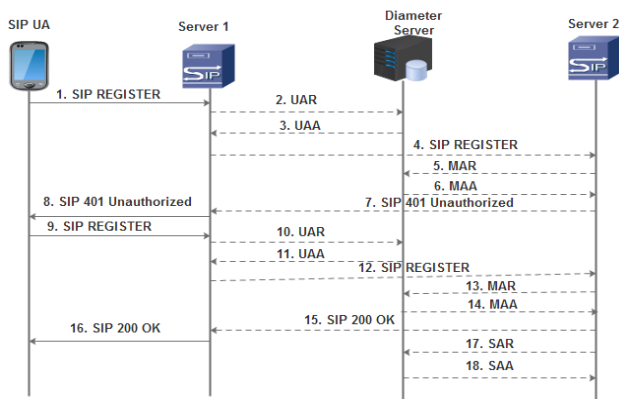


Figure 6. Registration Procedure Diameter SIP Application [RFC4740]

The diagram above does not work with certain architectures such as the IMS. The figure below shows the registration procedure (procedure) in IMS.

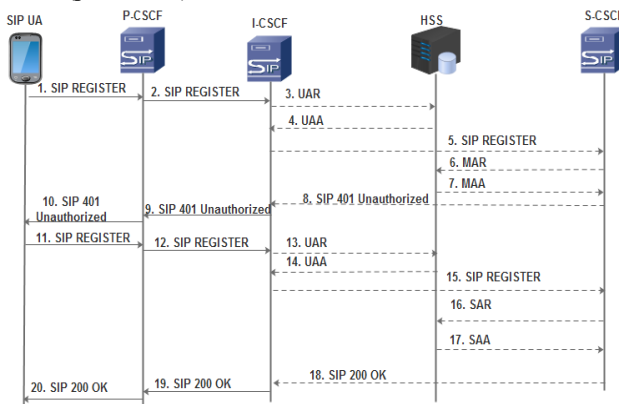


Figure 7. Procedure for Registration in IMS [RFC 4740]

The procedure for registering a user in the IMS network is written as follows:

1) The SIP UA provides its connection parameters in a SIP REGISTER request. This request contains the URI of its home network, its public and private identities and the address of the terminal from which it wishes to register. It then transmits the SIP REGISTER request to the CSCF Proxy on the Gm / SIP interface (step 1).

2) The Proxy-SCSF receiving the SIP REGISTER request adds the identifier of the visited network: P-Visited-Network-ID and a PATH header containing its URI, then transmits the request to the I-CSCF on the interface Mw / SIP (step 2).

3) The I-CSCF receives the SIP REGISTER request and the DIAMETER client requests the DIAMETER server through the DIAMETER SIP Application support to authorize to register by sending a User Authentication-Request (UAR) message. This message contains the AVPs, the SIP Address-O-Record (AOR) included in the SIP REGISTER request. The AOR contains the public and private identities plus the ID of the visited network. The DIAMETER server verifies the AOR SIP and, if it is a valid user defined in the home network, it allows the registration to continue (step 3).

4) The DIAMETER server responds with a DIAMETER User Authorization-Answer (UAA) message, which informs the DIAMETER client about the result of the user's permission. In the case of a successful authorization, the message DIAMETER UAA indicates the address of a local SIP server (in this case, it is the address of the S-CSCF entity) and / or list of capabilities that the I-CSCF server can use to select an appropriate S-CSCF server (step 4). When permission is successful, the I-CSCF sends the SIP REGISTER request to the S-CSCF server (step 5).

5) The DIAMETER client of the S-CSCF requests authentication parameters by sending a DIAMETER Multimedia-Auth-Request (MAR) message to the Diameter server. This request also makes the DIAMETER server aware of the SIP URI of the S-CSCF server in order to forward subsequent requests from the same user to the same server. The DIAMETER server responds with a DIAMETER Multimedia-Auth-Answer (MAA) message, which includes the SIP URI of the S-CSCF server, the user name, and other authentication vectors including the designated authentication algorithm associated with the user. Among other things, the MAA message includes a Digest-HA1 AVP that contains H (A1) as defined in RFC 2617 [12], and which allows the DIAMETER client to calculate the expected response. Then, the DIAMETER client can compare this expected response with the response to the challenge sent by the SIP UA. The absence of Digest-HA1 AVP in MAA indicates that authentication and authorization takes place in the DIAMETER server (steps 6 and 7).

6) The S-CSCF creates a SIP 401 response based on the challenges included in the MAA message, including the authentication hardware required by the SIP UA to include the appropriate credentials. The I-CSCF sends the request to the SIP UA client (steps 8, 9 and 10).

7) The SIP UA prepares a new SIP REGISTER request and transmits it to the P-CSCF, which relays the request to the I-CSCF. The I-CSCF receives the next SIP REGISTER request containing the user credentials (steps 11 and 12). Because it does not need to maintain a state, using SIP DIAMETER Application support, [10] it contacts the HSS (DIAMETER Server) server by sending a UAR message (step 13) to determine the S-CSCF server assigned to the user. The HSS responds by sending the SIP URI of the S-CSCF in a UAA message (step 14).

8) The I-CSCF sends the SIP REGISTER request to the S-CSCF server (step 15). The S-CSCF validates the credentials by comparing the response provided by the SIP UA with the expected response (based on the H (A1) received from the DIAMETER server).

9) If the credentials are valid, the S-CSCF sends a DIAMETER Server-Assignment-Request (SAR) message requesting that the HSS server confirm the completion of the authentication procedure and confirm the SIP URI of the S-CSCF which currently serves the user (step 16). The SAR message is also used to request that the DIAMETER server send the user profile to the S-CSCF server. The HSS responds with a DIAMETER Server-Assignment-Answer (SAA)

message. If the AVP value of the result code does not inform the S-CSCF of an error, the SAA message may include zero or more SIP-User-Data AVP containing the information that the S-CSCF needs to provide a service to the user. The S-CSCF inserts the profile of the user into a table called location (step 17).

10) Finally, the S-CSCF entity generates a "SIP 200 OK" response, which is sent to the I-CSCF server for eventual transmission to the SIP UA confirming the validation of the supplied parameters. The SIP UA is then recorded (steps 18, 19 and 20).

However, it must be noted that in step 16, the HSS server already displays "connected status" on its interface, while the user is not yet connected, because the S-CSCF has not yet downloaded the user's profile for storer in its location table (step 17) before generating the SIP 200 OK message that will be sent to the user to notify him that he is logged on.

E. KAMAILIO and IMS Modules

KAMAILIO is a project initiated by SER. This is a SIP server. As of version 4, KAMAILIO has integrated the IMS modules, which offers the possibility of using it as a platform to build an IMS core network.

According to 3GPP (3GPP 2005), IMS has become the standard for the use of voice and other multimedia services over LTE and other IP networks efficiently, securely and reliably, and then optional. It bridges the gap between circuit-switched voice services and IP-based technologies to open the voice to the development of multimedia services. IMS uses the SIP protocol for multimedia management. Many mandatory SIP extensions are built in to manage security and reliability. This management is implemented in the session control functions (CSCF).

Interactions between the various CSCF functions with elements such as PCRF, HSS, OCS and OFCS are performed using the DIAMETER protocol. DIAMETER is a protocol whose operation is based on AVP (Attribute-Value-Pair). It is responsible for managing authentication and authorization. Since IMS is based on open standards, it is easy to use provider platforms. KAMAILIO can be used as an IMS core, an IMS module like Proxy-CSCF can be used. The main KAMAILIO modules for IMS are described below:

1) *ims_auth*: this module is used for authentication in IMS. It supports MD5 and AKAv1 / 2 authentication schemes module est utilisé pour l'authentification dans IMS. Il prend en charge les schémas d'authentification MD5 et AKAv1/2

2) *ims_isc*: this module implements the IMS Service Control interface between the S-CSCF and the SIP AS

3) *ims_icscf*: module implementing the functions required to create an I-CSCF IMS. It can query a third party HSS to find the S-CSCF concerned for a request

4) *ims_qos*: this module implements the authorization functions between P-CSCF and PCRF.

5) *ims_registrar_pcscf*: This module simply implements the REGISTER processing logic for REGISTER messages in a P-CSCF configuration.

6) *ims_registrar_scscf*: this module simply implements the REGISTER processing logic for REGISTER messages in an S-CSCF configuration

7) *ims_usrloc_pcscf*: s the IMS equivalent of the KAMAILIO usrloc storage module. It stores the IMS subscriber information to the P-CSCF.

8) *ims_usrloc_scscf*: similar to the *ims_usrloc_pcscf* module, this module serves as a subscriber storage module for IMS subscribers to the S-CSCF.

9) *ims_ro_interface*: this module implements an online loading mechanism using the IMS DIAMETER Ro interface. The Ro interface is intended to be used in a KAMAILIO S-CSCF configuration and linked to an online loading system (OCS).

10) *AVP*: This module contains several functions that can be used to manipulate AVP content (Attribute-Value pairs). AVPs are variables attached to the SIP message being processed.

11) *CDP (C DIAMETER Peer)*: llows communication DIAMETER to and from KAMAILIO.

F. OpenIMSCore

OpenIMSCore is the implementation of an IMS core based on the open source SIP Express Router (SER). The main elements of the layer are: home subscriber servers (HSS) and various servers for call / session control (CSCF) functions. The control layer connects to the application servers (AS) in the service layer and to the user equipment (UE) via the transport layer. The Proxy-CSCF (P-CSCF) acts as the point of contact with the UE for access to the main network service; Interrogation-CSCF (I-CSCF) [8].

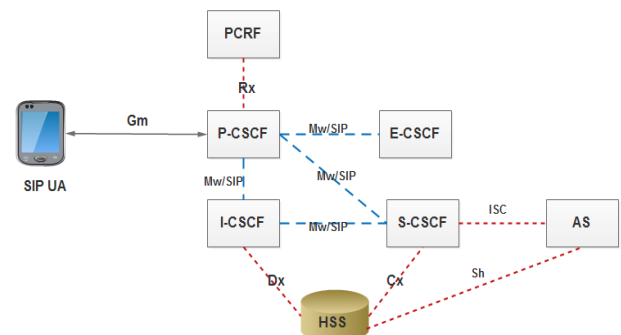


Figure 8. IMS network core entities

1) The P-CSCF is the entry point into the IMS network for all aspects of signaling a user's session. It is the point of contact between the user and the central server.

2) The I-CSCF constitutes, for a session of a user, the point of entry into the network of the operator to which the user has subscribed a service contract (SLA). It acts as an intermediary between the proxy server and the authentication server. It allows redirecting requests from a user to his original operator. The I-CSCF assigns a S-CSCF to the UE and transfers the request to the selected S-CSCF. To perform this function, an exchange of DIAMETER with the HSS entity is required. It

also generates the necessary information for the generation of tax receipts.

3) The S-CSCF is responsible for authenticating the user and providing operational services to him. It provides routing, billing information and maintains session status by controlling a timer (time), queries the HSS to check user rights against a service. At the same time, the S-CSCF records in the HSS the position of the subscriber in the network and informs the HSS of its address, so that an entity seeking to reach the subscriber knows which S-CSCF to address.

4) The HSS entity is a database that stores data specific to each user. The main recorded data include, among others:

- Table SVP (SerVice Profile): contains the service profile that is associated with each user
 - The public and private identities of the user (IMSU, IMPU and IMPI) with the other authentication and authorization information
 - Table Charging information (Chginfo): contains pricing information
 - Table Application Server (APSVR): contains the address of the AS to be contacted if the trigger points are compliant.
 - Table Initial Filter Criteria (IFC): which contains the initial filtering information, characterizing a certain service for the user. This table maps a point trigger that associates a point service set to an application server.
- 5) The E-CSCF entity is dedicated to the processing of emergency requests in the IMS network such as IMS emergency call sessions (toll-free numbers)
- 6) Table of different interfaces and entities.

Table 1. INTERFACES USED BY DIAMETER AND SIP

Entités	Interfaces	Protocols
Cx	Interface between CSCF and HSS	DIAMETER
Dx	Interface between SCSCF and SLF	DIAMETER
Gm	Interface between UE and P-CSCF	SIP
Isc	Interface between S-CSCF and AS (application server)	SIP
Sh	Interface between AS (SIP-AS or OSA-CSCF) and HSS	DIAMETER
Rx	-Interface between CRF and P-CSCF (Release 6) -Interface between PCRF and CSCF (Release 7)	DIAMETER
Mw	Interface between CSCFs	SIP

III. RESULTS AND DISCUSSION

All In this section, we present the platform used for the tests as well as the tools, techniques or methods.

A. Text

The figure below shows the test architecture we have set up.

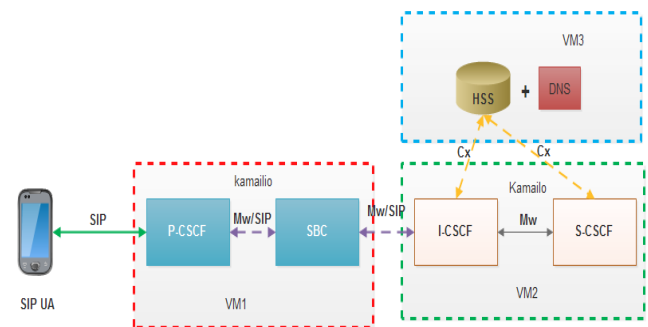


Figure 9. Test architecture

B. Results

The results presented below are intended to describe the procedure for registering users in the IMS network. These results are based on the tests carried out and the analysis of the different DIAMETER messages exchanged between the HSS, I-CSCF and S-CSCF entities in order to highlight the reliability problem of the HSS data.

We tried to register a user from an IMS Boghe client. The HSS entity associates to the user the appropriate S-CSCF entity (see Figure 10). In step 16 (Figure7), the HSS already associates the Serving-CSCF (identity provided in the Diameter SAR message) which deserts the use.

IMS Subscription - Search Results

ID	Name	S-CSCFName	Diameter Name
1	alice	sip.scscf.lirt.sn:6060	scscf.lirt.sn
2	bob		
3	yvan		
5	dany	sip.scscf.lirt.sn:6060	scscf.lirt.sn

Rows per page
1 20

Figure 10. Selection of the S-CSCF by HSS of a user

This is step 17 (Figure 7) where the HSS has received the SAR message in which the S-CSCF has sent its parameters to it by requesting to send it a part or the entire profile of the S-user in the Diameter SAA message. At this time, the HSS already displays on its interface that the user is connected (see Figures 11, 12 and 13).

Public User Identity - Search Results

ID	Identity	Implicit-Set ID	Type	Reg. Status	Barring
1	sip:alice@lirt.sn	1	Public_User_Identity	Not-Registered	false
2	sip:bob@lirt.sn	2	Public_User_Identity	Not-Registered	false
3	sip:dany@lirt.sn	3	Public_User_Identity	Registered	false

Rows per page
1 20

Figure 11. Viewing HSS Connected Users

Public User Identity -IMPU-

ID	3
Identity*	sip:dany@lirt.sn
Barring	☐
Service Profile*	default_sp
Implicit Set	3
Charging-Info Set	default_charging_set
Can Register	☒
IMPU Type*	Public_User_Identity
Wildcard PSI	
PSI Activation	☐
Display Name	
User-Status	REGISTERED

Mandatory fields were marked with "**"

Add Visited-Networks

Select Visited-Network...

List of Visited Networks

ID	Identity	Delete
1	lirt.sn	☐

Associate IMPI(s) to IMPU

IMPI Identity

Warning: This IMPI will be associated with all the cc IMPUs (within the same implicit-set)!

Figure 12. Viewing the user profile

```

defaultHandling></ApplicationServer></InitialFilterCriteria></ServiceProfile></IMS
SSubscription>
2017-10-13 01:52:36,324 INFO de.fhg.fokus.hss.cx.op.SAR - processRequest
User with Public Identity: sip:dany@lirt.sn and all its corresponding implicit-se
t identities are Registered!
2017-10-13 01:52:36,446 DEBUG de.fhg.fokus.hss.main.Task - execute Processing LI
R!
2017-10-13 01:53:23,224 DEBUG de.fhg.fokus.hss.main.Task - execute Processing LI
R!

```

Figure 13. User subscription at HSS

However, on the HSS system log interface, we find that it did not send the expected SAA response from the SAR message. Having failed to receive the user profile (transmitted in the SAA message), the S-CSCF could not store the user profile. Therefore, it did not send the expected response "SIP 200 OK" to notify the user that it has logged on. On the client interface, we see that the user is not logged in. Figure 14 shows the user terminal interface.

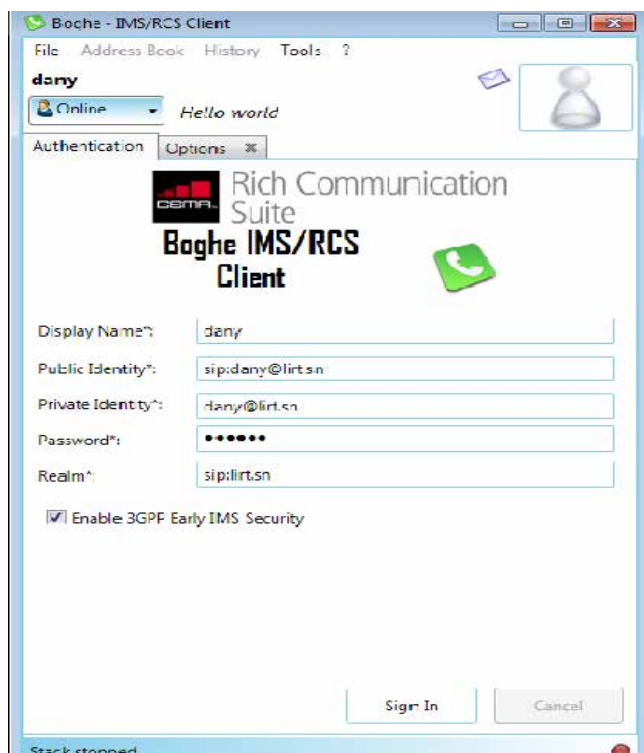


Figure 14. User Terminal Interface

We have analyzed the frames below to observe the exchanges between the different entities during the registration process.

```

Session Initiation Protocol (403)
  Status-Line: SIP/2.0 403 Forbidden - HSS Identity not registered
    Status-Code: 403
    [Resent Packet: False]
    [Request Frame: 5473]
    [Response Time (ms): 66]
  Message Header
  Via: SIP/2.0/UDP 192.168.43.4:54872;received=192.168.43.4;branch=z9hG4bK267635647;rport=54872
    Transport: UDP
    Sent-by Address: 192.168.43.4
    Sent-by port: 54872
    Received: 192.168.43.4
    Branch: z9hG4bK267635647
    RPort: 54872
  From: <sip:dany@lirt.sn>;tag=266899826
    SIP from address: sip:dany@lirt.sn
    SIP from tag: 266899826
  To: <sip:dany@lirt.sn>;tag=0611027e96ab28c6b5bc2bb22d130006-e579
    SIP to address: sip:dany@lirt.sn
    SIP to tag: 0611027e96ab28c6b5bc2bb22d130006-e579
    Call-ID: dc899bed-bec9-39e9-c41c-a809cbf91007
  CSeq: 22930 REGISTER
    Sequence Number: 22930
    Method: REGISTER
    Server: Kamailio I-CSCF
    Content-Length: 0

```

Figure 15. Frame capture at the I-CSCF

Figure 16 shows a frame capture performed at the level of the S-CSCF. Based on this frame, we note that the S-CSCF did not send the "SIP 200 OK" response as it did not store the user's profile.

```

Session Initiation Protocol (200)
  Status-Line: SIP/2.0 200 Subscription to REG saved
    Status-Code: 200
    [Resent Packet: False]
    [Request Frame: 2746]
    [Response Time (ms): 5]
  Message Header
  Record-Route: <sip:mo@192.168.43.141;lr=on;ftag=266909853;vst=AAAAAAAAAAAAAAAAAAAA-->
  Via: SIP/2.0/UDP 192.168.43.4:54872;received=192.168.43.4;branch=z9hG4bK266913671;rport=54872
    Transport: UDP
    Sent-by Address: 192.168.43.4
    Sent-by port: 54872
    Received: 192.168.43.4
    Branch: z9hG4bK266913671
    RPort: 54872
  From: <sip:dany@lirt.sn>;tag=266909853
    SIP from address: sip:dany@lirt.sn
    SIP from tag: 266909853
  To: <sip:dany@lirt.sn>;tag=0dd96c3f57e2a45170b08bd38407c6fd-5c5d
    SIP to address: sip:dany@lirt.sn
    SIP to tag: 0dd96c3f57e2a45170b08bd38407c6fd-5c5d
    Call-ID: 08de0701-7deb-1162-0504-9fabf22099f8
  CSeq: 24466 SUBSCRIBE
    Sequence Number: 24466
    Method: SUBSCRIBE
    Expires: 600000
  Contact: <sip:scscf.lirt.sn:6060>
    Contact URI: sip:scscf.lirt.sn:6060
    Contact URI Host Part: scscf.lirt.sn
    Contact URI Host Port: 6060
  Server: Kamailio S-CSCF
  Content-Length: 0

```

Figure 16. Frame capture at the S-CSCF level

Following the various tests carried out above which highlight the problem of registration of the user, we propose the improvement solution below:

a) Record diagram layout integrating the queue manager:

Based on the IMS registration procedure (Figure 7), we propose the following registration diagram by integrating two Rabbitmq servers in it, which will interact with the I-CSCF, S-CSCF and the HSS.

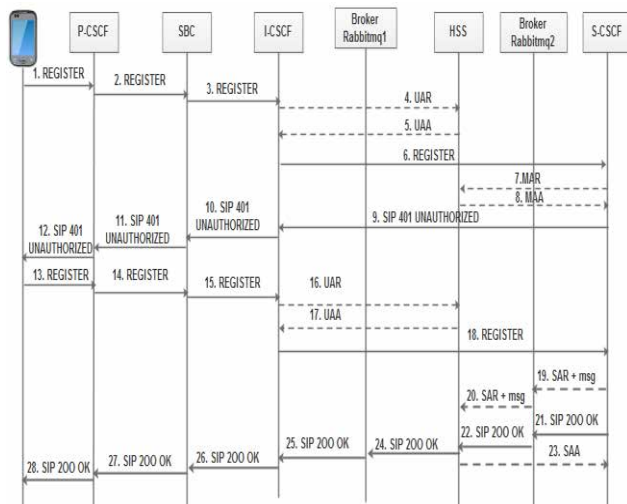


Figure 17. Proposal of the registration procedure diagram in IMS

Referring to Figure 6, steps 1 through 18 are identical. In the diagram shown in Figure 17, two Rabbitmq Brokers were integrated into the diagram. When the S-CSCF receives the REGISTER message, it triggers the sending of a DIAMETER SAR message plus another message to instruct the HSS to wait for the SIP 200 OK message to be received before sending the SAA message. The S-CSCF also triggers the sending of the SIP 200 OK message (step 21) which will be transmitted to the Broker Rabbitmq2 which will then be sent to the HSS. The HSS will retransmit the SIP 200 OK message to the Rabbitmq1 Broker which transmits it to the CSCF for the user. Upon receipt of the SIP 200 OK message, the HSS responds by sending the DIAMETER SAA message containing part or profile of the user. At this time, it can associate with the user's profile the URI of the S-CSCF that serves it and at the same time displays the "connected status". The S-CSCF will then stoker in its location table the profile of the user who wishes to register. Above the architecture of the proposed solution.

b) Architecture of the proposed solution

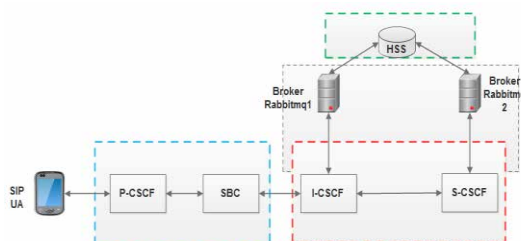


Figure 18. Architecture of the HSS solution with Rabbitmq

IV. CONCLUSIONS AND PERSPECTIVES

The HSS entity is a central element in the converged telecommunications system. It is important that it function normally so that the exchanges of user data with the other entities of the IMS network are reliable.

We used the IMS KAMAILIO and OpenIMSCore modules to demonstrate the HSS malfunction. To solve this malfunction, we introduced the Rabbitmq queue manager to improve the exchange of information.

In future work, it would be important to carry out full-scale tests to see the effect of integrating this queue manager into system performance and quality of service. Use of queue modeling tools will help to achieve this.

ACKNOWLEDGMENT

The authors would like to thank the LIRT Laboratory Manager for the help he provided during the research.

REFERENCES

- [1] *An Introduction to LTE : LTE, LTE-Advanced, SAE, VoLTE and 4G Mobile Communications*, Second Edition. Christopher Cox. © 2014 John Wiley & Sons, Ltd. Published 2014 by John Wiley & Sons, Ltd..
- [2] André Pérez. (2013) *La voix sur LTE: réseau 4G et architecture IMS*, ISBN 978-2-7462-4546-4 © 2013, Lavoisier, Paris.
- [3] Poikselkä, M., Holma, H., Hongisto, J. et al. (2012) *Voice over LTE (VoLTE)*, John Wiley & Sons, Ltd, Chichester.
- [4] Christina Gessner, Rohde & Schwarz, "Long Term Evolution – A concise introduction to LTE and its measurement requirements", ISBN 978-3-939837-11-4.
- [5] Camarillo, G. and Garcia-Martin, M.-A. (2008) *The 3G IP Multimedia Subsystem (IMS): Merging the Internet and the Cellular Worlds*, 3rd edn, John Wiley & Sons, Ltd, Chichester.
- [6] Noldus, R., Olsson, U., Mulligan, C. et al. (2011) *IMS Application Developer's Handbook: Creating and Deploying Innovative IMS Applications*, Academic Press.
- [7] Jih-Wei Tsai*, Chao-Chun Huang, Chih-Sheng Chang, Chung-Shih Tang, Chin-Ywu Twu; "The Technique of IMS Sh Interface and its NGN LBS Application" *Broadband Network Technology Lab. Telecommunication Laboratories, Chunghwa Telecom Co., Ltd. Taiwan, R.O.C.*
- [8] Imène ELLOUMI, 2012. "Management of mobility between access networks and Quality of Service in an NGN / IMS approach." Thèse doctorat: University of Carthage (Tunisie).
- [9] "Diameter Request for comments 6733" (RFC-6733) [Online]. Available: <http://www.tools.ietf.org/html/rfc6733>.
- [10] Open Diameter Project, Open Diameter Home Page. [Online]. Available: <http://www.opendiameter.org/>
- [11] "Diameter SIP Application 4740" (RFC-4740) [Online]. Available : <http://www.tools.ietf.org/html/rfc4740>
- [12] IETF "HTTP Authentication: Basic and Digest Access Authentication 2617" (RFC-2617) [Online]. Available: <http://www.tools.ietf.org/html/rfc2617>.
- [13] "Cx and Dx Interfaces Based on the Diameter Protocol (Release 11)", 3GPP TS 29.229–2011, 2011.
- [14] Liang Xu1, Changcheng Huang1, James Yan1 and Tadeusz Drwiega2, "De-Registration Based S-CSCF Load Balancing in IMS Core Network1", 1 Department of Systems and Computer Engineering, Carleton University, Ottawa, Canada 2 Nortel Networks, Ottawa, Canada {liangxu, huang}@scc.carleton.ca, jim.yan@sympatico.ca, drwiega@nortel.com
- [15] SRIHARSHA C, Prof. SANDHYA S, "Role of DiameterStack Protocol in IMS NetworkArchitecture"(IJITR) INTERNATIONAL JOURNAL OF INNOVATIVE TECHNOLOGY AND RESEARCH Volume No.3, Issue No.3, April - May 2015, 2180 – 2183.Bangalore, India.



Ngartabé KAG-TEUBE, Telecommunication engineer, Master in teleinformatics. He is currently working at ASECNA as an expert in radionavigation and satellite communications (IBS, VSAT-VHF Remote). He is currently a doctoral student at the Computer, Networks and Telecoms Laboratory (LIRT) at the Cheikh Anta Diop University of Dakar. His research is focused on multimedia services.



Yvan P. KALIA-SYA D. is a Telecommunications and Networks Engineer, certified Linux, Cisco and Novell. He teaches at the Higher Polytechnic School of CHEIKH ANTA DIOP University. He obtained his Master 2 degree in Telecommunications and Networks and applications based on Free Software at the Central School of Free Software and Telecommunications of Dakar. He did his master's degree in engineering science on Modeling and Simulation of Complex Systems at the Polytechnic School of CHEIKH ANTA DIOP University. He has expertise in extensive networks and operator. He was technical manager at the operator HAYO telecoms (Senegal). He worked on multimedia NGN architectures in the NGN laboratory of the RTN-EC2LT group (Networks and Digital Techniques - Central School of Free Software and Telecommunications).



Pr. Samuel Ouya is currently the Director of Computer, Network and Telecom Laboratory (LIRT) at University Cheikh Anta DIOP of Dakar. He was from 2013 to May 2017 the first Director of Infrastructure and Information System of the first virtual university of Senegal (UVS). Holder of a Thesis in Applied Mathematics from the Gaston Berger University of Saint-Louis in Senegal and a Telecommunications Thesis from the Cheikh Anta Diop University (UCAD) in Dakar-Senegal, he is interested in Applications of innovative telecom services to virtual organizations and IoT.



Kéba GUEYE is currently a PhD student at Computer, Network and Telecom Laboratory (LIRT) at University Cheikh Anta DIOP of Dakar. Holder a Master's degree in Research "Physics and Application: specialization on Electronics – Systems - Telecommunication" from the University Cheikh Anta Diop (UCAD) of Dakar-Senegal. His current research interests include Internet of Things IoT and Intelligent System, VoLTE, CoAP, MQTT.