AAA architectures applied in multi-domain IMS (IP Multimedia Subsystem)

W.S. Ooms, G. Karagiannis
Design and Analysis of Communication Systems,
Department of Electrical Engineering, Mathematics and Computer Science, University of Twente,
Enschede, the Netherlands
w.s.ooms@alumnus.utwente.nl, g.karagiannis@utwente.nl

M.O. van Deventer, J. Veldhuizen
Netherlands Organisation for Applied Scientific Research – Information and Communication Technology (TNO-ICT),
Delft, the Netherlands
Oskar.vandeventer@tno.nl, Jurjen.veldhuizen@tno.nl

Abstract— **There is a group of communication services that use resources from multiple domains in order to deliver their service. Authorization of the end-user is important for such services, because several domains are involved. There are no current solutions for delivering authentication, authorization and accounting (AAA) to multi-domain services. In our study we present two architectures for the delivery of AAA to such services. The architectures are analyzed on their qualitative aspects. A result of this analysis is that direct interconnection of AAA servers is an effective architectural solution. In current multi-domain IP Multimedia Subsystem (IMS) architectures, direct interconnection of AAA servers, such as the Home Subscriber Servers (HSS), is not yet possible. In this paper we argue and recommend to extend the IMS specification by adding a new interface to HSS in order to support the direct interconnection of HSS/AAA servers located in different IMS administrative domains.**

IMS, AAA, UMTS, HSS, security, multi-domain

I. INTRODUCTION

A special category of communication services are the ones that use resources from multi-domains in order to deliver their service. Interaction between the domains is necessary to support and deliver the service. There are different examples of such communication services that are distributed over multiple domains.

The first example is a carrier pre-select service [1]. With carrier pre-select a user can decide to make a part of its telephone calls over the network of the carrier pre-select service provider. For example international calls can be routed via the network service provider to the carrier pre-select service provider that offers a better price. The network service provider is the provider who offers the network access to the end-user. The carrier pre-select provider also has an accounting relationship with the end-user. The carrier pre-select service is distributed over several domains, because the network service provider uses resources to route the call and the carrier pre-select service provider also supplies resources. In Figure 1(a) the relation between the different parties is shown. The end-user has accounting relationships with the network service provider and the carrier pre-select service provider. The network service provider and carrier pre-select service provider have a relationship between their domains for the service delivery.

The second example is a service called FoneFreez™ [2]. It provides service interaction between an IPTV (IP TeleVision) service and an IP telephony service. The elementary service interaction between them is as follows: when watching television the phone rings, if the phone is picked-up the television service pauses and starts recording. After the conversation the television program continues where it was stopped. This service makes sure that the user does not miss anything of his/her favorite television show. The advantage of FoneFreez is that services can be reused, and does not need to be rebuilt when service interaction is added. The relations between the different parties are shown in Fig. 1(b). The end-user has an accounting relationship with the telephony and television service providers. Both service providers are interconnected to enable the service delivery.

When these distributed services are used, multiple parties supply resources to enable full service delivery. An essential property of the kind of multi-domain service interaction described in these examples is that there are at least two parties that have an accounting relationship with the end-user. This results in different customer identities under which the end-user is known at the service providers. Authorization of the end-user is necessary at all domains to permit the usage of the resources by a specific end-user. Such multi-domain services can be applied in IP Multimedia Subsystem (IMS) architectures. IMS [3], [4], [17] is a standardized framework typically used by telecom operators to provide mobile and fixed multimedia services in an all IP environment. In order to

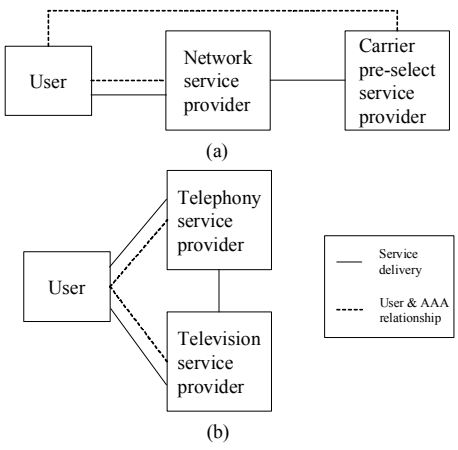

Figure 1 Examples of multi-domain services

provide authentication, authorization and accounting (AAA) services in IMS networks typically the AAA architecture and framework is used [5], [6]. The main challenge related to the use of the AAA architecture for multi-domain services, which is not previously described in literature, is the fact that the scenario where one user has several accounting relationships for one service that crosses multiple domains is not taken into account.

IMS uses the AAA architecture and framework for the support of authentication, authorization and accounting services. The main challenge related to the integration of the multi-domain AAA architecture and IMS, is the fact that currently, the IMS architecture is developed to run in a single administrative domain under management of one party. Therefore it is not possible to split the IMS architecture and divide it over multiple administrative domains that are managed by different parties.

In this paper two main research questions are answered.

1) How can AAA be provided for multi-domain services?
2) How can the multi-domain AAA architecture be integrated in the IMS architecture?

This paper is organized as follows. Section II describes the related research in the field of IMS, identity management and AAA architectures. Section III describes the research methodology used for our study. In Section IV two different solutions are presented. Section V gives an analysis of the results. The application of the AAA solutions in multiple IMS administrative domains is described in Section VI, followed by the conclusion and further research topics.

II. RELATED RESEARCH

In [7] different generic AAA architectures for authorization are presented. Primarily there are three different message sequences distinguished for authorization of the end-user by a service provider: agent sequence (Fig. 2a), push sequence (Fig. 2b) and pull sequence (Fig. 2c) Authentication and accounting were out of scope of [7].

In the agent sequence scenario, see Fig. 2(a), the user contacts the AAA entity first. The AAA server authorizes the user, and the service equipment is notified. The service equipment can set up the service and notifies the AAA server that it is ready, which subsequently notifies the user. The user and service equipment can precede the communication directly, without the AAA server functioning as an agent. An example of this situation is when a user requests Internet access. The user is first connected to the AAA server of the internet service provider. When the AAA server has authenticated the user, the proxy of the service provider is notified and the connection is established.

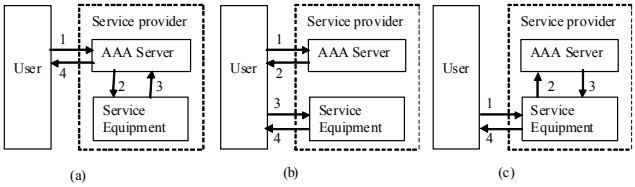

Figure 2 Agent, push and pull sequence [7]

In the push sequence scenario, see Fig. 2(b), the user directly requests the service from the service equipment, which authorizes the user by placing a request at the AAA server. An example of this situation is when a user pays with his/her credit card and the store checks with the credit card company if the card is still valid.

In the pull sequence scenario, see Fig. 2(c) the user receives a token from the AAA server with which the user can request the service and prove that it is authorized to use the service. An example of this situation is the case where a user is going to the theater. First the user buys a ticket at the box office. Before entering the auditorium the attendant requests from the user his/her ticket, which it proves that the user has paid.

These AAA architectures consider multiple domains, but the situation where several accounting relationships of an end-user exist in one service that crosses multiple domains is not described. Furthermore, the current AAA architecture is not able to efficiently support the federation of identities where the user is known under multiple identities at the service. A federation of identities is a group of organizations or systems that exchange identity information in a secure way. An initiative where identity federations are described is Liberty Alliance [8]. Most of the work of Liberty Alliance is focused on single-sign-on. It is a method of access control that enables an end-user to authenticate once and gain access to the resources of multiple software systems, and not need to authenticate again. However, the federation of identities where the user is known under multiple identities at the service is not specifically regarded in the work of Liberty Alliance.

IMS is an architectural framework that is among others used in the 3GPP (GSM (Global System for Mobile communications) and UMTS (Universal Mobile Telecommunication System)) architecture [3]. The framework, see Fig. 3, consists of a transport plane, control plane and application plane. In every plane several functional entities are defined, see [17], [9].

The application plane contains application and content servers that run value added services for users. The Service Capability Interaction manager (SCIM) provides an interface to

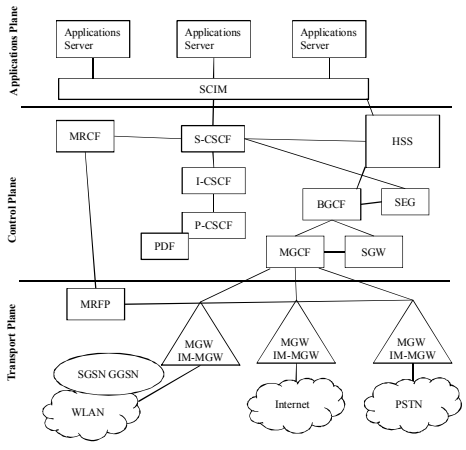

Figure 3 Simplified IMS reference architecture [9]

the control plane to enable combinations of the applications that run on the application servers. The control plane contains different functions like the Home Subscriber System (HSS), Call Session Control Function (CSCF) and border gateways (BGCF) that control calls and sessions, Media Resource Function Controller (MRFC), and support functions like provisioning and charging. The transport plane consists of Media Gateways (MGW), routers and switches for the backbone and access networks, both fixed and mobile. Different IMS administrative domains can be interconnected through the Security Gateways (SEG). The CSCF handles the call and functions as a SIP server. The CSCF is decomposed in different types of session control functions: serving (S-CSCF), interrogating (I-CSCF) and proxy (P-CSCF) call session control functions. The Home Subscriber Server (HSS) is an important entity in IMS when considering the support of AAA services. In the HSS user profiles are stored, and authentication and authorization is done for the end-user. Therefore, the HSS is considered to be the AAA server.

In IMS administrative domains only one customer relation is presumed. Currently, there are no cases supported where an end-user has multiple identities with multiple service providers for a single IMS service experience. This is due to the manner of how the user is registered in the HSS. In roaming situations the HSS is contacted with which the user has an accounting relationship. Multiplicity of identities is used in IMS for users that have multiple devices or profiles. Currently there are no possibilities in the IMS specification for supporting AAA for multi-domain service interaction.

III. Research Methodology

Different research methods are used in order to answer the research questions listed in section I.

The first research method used is a case study [10] of the FoneFreez case [2]. With the help of TNO-ICT experts a scenario of AAA for FoneFreez was drawn up. Second, the scenario based requirements elicitation research method [11] is used to derive requirements from the scenario. The requirements are divided in four different categories: functional requirements, non-functional requirements, constraints and acceptance criteria. The functional requirements describe the behavioral aspects of the solution, the non-functional requirements describe some of the performance aspects. The constraints are requirements that must be met. The acceptance criteria are used to differentiate and compare the alternative solutions. It is important to note that in the M. Sc. Thesis report of W. Ooms [2], more details can be found on the used research methodology.

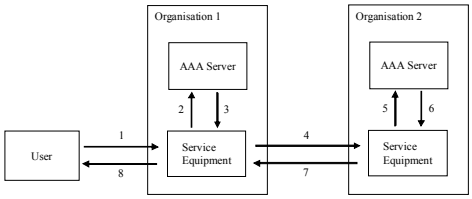

Figure 4 Hop-by-hop AAA solution

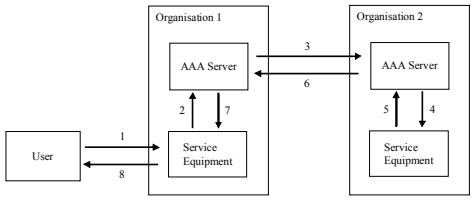

Figure 5 End-to-end AAA solution

For the provisioning of AAA, a protocol is needed that is able to provide AAA over multiple domains. In our research we chose the Diameter protocol [12], the successor of the RADIUS protocol. One of the motivating arguments to choose the Diameter protocol was related to the fact that according to its specification it should be able to handle certain AAA services over multiple administrative domains. Another motivating argument was to find out the application area of this relatively new protocol, which is already adopted in IMS. For the design, the concepts found in literature, see Section II, are used as much as possible. In order to distinguish the different design phases the method described in [13] is used. We distinguished three design phases; initialization phase, log-on phase and operational phase. These phases are used to refine the aspects that the solution has to solve. Alternative solutions are compared using the acceptance criteria, followed by the verification of the fulfillment of the requirements.

IV. Solutions and Results

This section describes two solutions of how AAA architectures can be implemented in real multi-provider settings. Three phases could be distinguished for each solution. The initialization phase, where the connections and trust between the different parties are established, and identities are exchanged. In this phase the user registers and the AAA architecture must check whether the user is also known at the service providers for which the interaction will take place. Because the user is known under different identities at the different parties, exchange with respect to the privacy of the end-user must be arranged. The second phase, i.e., log-on phase, occurs every time the user starts the service. In this phase the authentication, authorization and accounting for the end-user must be done. The third phase represents the normal behavior of the service. Accounting and possibly re-authentication takes place during this phase. Our solution on providing AAA is the application of the AAA architectures presented in [7], to situations where two or more simultaneous accounting relationship with the same end-user exist, when all relationships use their own authentication credentials and identities. This resulted in the derivation of two different architectures: "hop-by-hop AAA solution" and "end-to-end AAA solution".

The "hop-by-hop AAA solution", see Fig. 4, is a repetition of the pull sequence as described in Fig. 2(c), while the "end-to-end AAA solution", see Fig. 5, is the combination of the pull (Fig. 2(c)) and agent sequence (Fig. 2(a)).

In the "hop-by-hop AAA solution" the authentication of the end-user, during the log-on phase of the interaction service, occurs per each domain. Each domain can arrange its own AAA, and then it forwards the request to the next domain. The interactions are also shown in Fig. 4. The interactions 2,3 and 5,6 are accomplished using the Diameter protocol. In the "end-to-end AAA solution", the AAA servers are interconnected with the Diameter interfaces. During the log-on phase, the AAA servers authenticate the end-user and forward the request to the next domain. Fig. 5 also shows the interactions during the log-on phase, for the "end-to-end AAA solution". Here the interactions 2 to 7 are accomplished using the Diameter protocol.

V. ANALYSIS

Both alternative solutions can be realized using the Diameter protocol and are analyzed using acceptance criteria. This is due to the fact that DIAMETER [12] supports proxying and redirecting of authentication information. The NASREQ Diameter application [14] can be reused in its existing form, to provide the authentication, authorization and accounting functionality needed. Because of the flexibility and roaming capabilities of the protocol, the specification can be reused without the need of extension or alterations. Table I presents the criteria and the qualitative performance of both solutions on the different parts. The fulfillment ranges from -- to ++.

TABLE I. COMPARISON SPECIFICATIONS

No.	Qualitative performance		
	Acceptance criteria	*Hop-by-hop*	*End-to-end*
1	Extendable, more operators and more applications can be added	+	++
2	Level of trust between domains	+	++
3	Minimal number of components that are needed to realize the architecture	+	-
4	Minimal number of interactions/packets between realms	-	+
5	No/minimal alterations to the Diameter specification	++	+
6	Easy identity management – exchanges of identities	-	+
7	Reuse of Diameter architecture in services that are based on IMS	-	--

The acceptance criteria are satisfied by the two AAA solutions in the following way:

Acceptance criterion (1): Because the "end-to-end AAA solution" uses standard interfaces to connect the entities from different domains, adding more applications or more administrative parties is easy. In these situations the "hop-by-hop AAA solution" requires additional configuration updates for the service equipment.

Acceptance criterion (2): The "end-to-end AAA solution" uses the Diameter messages to establish a security association between entities from different domains. This concept is used in the Diameter Mobile IPv4 application [15]. The "hop-by-hop AAA solution" for its security depends on other protocols like Kerberos [16] to establish a secure connection between the entities. It is not explicitly that the level of trust is higher in one solution or the other, but that it is easier realized. In the "end-to-end AAA solution", trust is enhanced during the authentication procedure and no other messages are needed for this procedure. The "hop-by-hop AAA solution" uses the Kerberos protocol to authenticate the devices located on the different domains, but it also needs messages for authentication of the end-user in the different domains.

Acceptance criterion (3): The "hop-by-hop AAA solution" needs less interfaces than the "end-to-end AAA solution", because the interfaces between the AAA servers are left out in the current AAA specification.

Acceptance criterion (4): The number of packets required during the operational phase is the same in both solutions. The "end-to-end AAA solution" has the advantage that authentication and authorization between the entities can be accomplished in parallel with other messages required for normal operation, via the AAA architecture. This can be an advantage when the user is re-authenticated, and no delay is added to the regular process. The number of interactions needed in the two solutions is different during the log-on phase, see [2]. In the "end-to-end AAA solution" the Diameter interface added, is a standard interface, while the interface in the "hop-by-hop AAA solution" becomes more complex, due to the fact that in addition to eight Diameter messages, see [2], needed in the "hop-by-hop AAA solution" also six application specific messages are needed. In the "end-to-end AAA solution" eight Diameter messages are sufficient, see [2].

Acceptance criterion (5): For both solutions, the Diameter specification does not require alterations. The "hop-by-hop AAA solution" is easiest to implement, because only messages are exchanged between a client and server of a particular domain. The "end-to-end AAA solution" requires the service equipment to know which Diameter requests to send. However, the forwarding of the messages to different domains by the AAA servers is already included in the Diameter specification.

Acceptance criterion (6): The exchange of identities is easier when the parties that maintain the identity of the user are interconnected as provided in the "end-to-end AAA solution". A federation can be built between the parties as done in Liberty [8]. For identity management in the "hop-by-hop AAA solution", the federation must be built between the domains, and the entities must be concerned with the management of the identities of the user. This results in more configuration requirements on the used entities.

Acceptance criterion (7): The only criterion that the "end-to-end AAA solution" specification fails to fulfill is the reuse of the Diameter architecture when one or more administrative parties use an IMS network. In the "hop-by-hop AAA solution" the inter-connection between IMS administrative domains can be done using Security Gateways (SEG), see Section II. The end-to-end specification is based on an interconnection of the AAA servers. In IMS the AAA server is the HSS, meaning that if the "end-to-end AAA solution" is used then the HSS (AAA server) located in one IMS administrative domain should be able to be interconnected with another HSS (AAA server) that is located in another IMS administrative domain via an

DIAMETER interface. The current IMS specification does not support this HSS interface.

It is important to note that the M. Sc. Thesis report of W. Ooms [2] discusses and shows that both alternative solutions that are introduced in Section IV fulfill the functional requirements, non-functional requirements and the constraints. Due to the above fact and due to the fact that the available number of article pages is limited, the analysis based on the above listed requirements is not presented in this paper, but it can be found in [2].

VI. Application of AAA in multi-domain IMS

In IMS several interfaces to the HSS are defined that use the Diameter protocol (Cx, Sh) [17]. The HSS is the AAA server of an IMS administrative domain, which authenticates and authorizes the user and stores the user profiles. The interfaces transport authentication and authorization information from service equipment, which contain AAA clients like application servers and CSCF, to the HSS, see Section II. Specific applications of Diameter are defined for these interfaces. In Fig. 6 the application of the multi-domain AAA in IMS and non-IMS administrative domains is shown. In the IMS domain, the HSS is considered to be the "AAA server" and the IMS core and application servers are considered to be the "Service equipment".

The IMS core and application servers contain multiple AAA clients that communicate with the HSS. As shown in Section II, the IMS architecture is much more complex and consists of more components, see [17]. To enable services that cross multiple domains, the HSS will need to use extra information to supply the correct authentication and authorization. The HSS provides AAA for the users that are registered within an IMS administrative domain. If another administrative domain is involved, then that domain should handle its own AAA interactions. In the current IMS specification, the "hop-by-hop AAA solution" can be easily implemented. IMS administrative domains can already be interconnected. The IMS core & application servers (i.e., service equipment) belonging to different administrative domains are connected according to the "hop-by-hop AAA solution", see Fig. 4. In the current IMS specification, the "end-to-end AAA solution", see Fig. 5, is not possible because the HSS does not support an interface that can be used for the interconnection to other HSSs (AAA servers). Based on the analysis presented in Section V, it can be concluded that it is advantageous to add an interface to HSSs that can be used for their interconnection to other HSS/AAA entities located in different IMS administrative domains. Note that this interface can also be used to interconnect a HSS/AAA entity located in an IMS administrative domain to an external AAA server located in a non-IMS administrative domain, see Fig. 6. Currently the 3GPP standardization body does not specify an interface for the multi-domain interconnection of HSS AAA servers. Therefore, we argue and recommend that such a multi-domain interconnection interface for the HSS AAA should be added in the IMS specification. Due to the fact that the Diameter protocol is already used in IMS, adding and implementing an extra Diameter interface to HSS is considered to be simple.

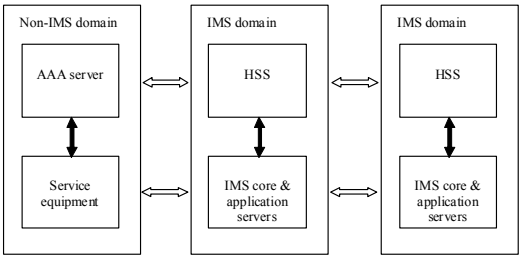

Figure 6 Multi-domain AAA in IMS and non-IMS domains

VII. Conclusion and further research

This paper presents several concepts that are applied in AAA and IMS architectures used in multiple administrative domains. In particular this paper answers the following two main research questions:

1) How can AAA be provided for multi-domain services?
2) How can the multi-domain AAA architecture be integrated in the IMS architecture?

Two AAA solutions that can be used in multiple administrative domains are proposed, the "hop-by-hop AAA solution" and the "end-to-end AAA solution". Based on several acceptance criteria it could be concluded that the "end-to-end AAA solution" outperforms the "hop-by-hop AAA solution". However, further research can be done in order to compare these solutions based on quantitative performance criteria, such as scalability and end-to-end signaling mean delays. The only disadvantage of the "end-to-end AAA solution" is related to the fact that it cannot be applied in the current IMS specification. This is because the AAA server, which is the HSS entity in the IMS specification, does not support an interface that can be used for the interconnection to other HSS (AAA) entities. There are several reasons to be careful with an extra interface to the HSS. In the HSS the user profiles are stored. This is privacy sensitive information and must be secured to a great extent. An extra interface especially from a non-IMS administrative domain can be a security threat. Furthermore the HSS is a database and agreements must be made on how information can be extracted from this database. With the "end-to-end AAA solution", an interface must be defined using a standard protocol like Diameter. This protocol is secure and agreements about extracting information can be arranged. The advantage is that faster authentication is possible and identities can be easily managed when a standard interface is designed. The complexity of connection to another network can be reduced, by using the Diameter protocol on an end-to-end basis. The Diameter protocol is already used in IMS, which makes adoption of an extra Diameter interface easier. Further research should be done on the HSS interface that is used to interconnect an IMS administrative domain with an AAA server located in a non-IMS administrative domain. The exchange of identities can be done in several ways, which way is best suited should be further explored.

ACKNOWLEDGMENT

We would like to acknowledge the following colleagues for reviewing the research study and the previous versions of the paper and providing useful comments: Aiko Pras, Hans Stokking, Fabian Walraven, Mike Schenk, Frank Fransen, George Huitema, Henk Ensing, Frens Rumph, Johan Boekema, and Klaas Wierenga.

REFERENCES

[1] "Study on the Cost Allocation for Number Portability, Carrier Selection and Carrier Pre-Selection", Final Report for DGXIII of the European Commission, Europe Economics & Arcome, Volume I, October 1999

[2] Ooms, W., "Providing AAA with the Diameter protocol for multi-domain service interaction", Masters thesis, University of Twente, 2007, http://dacs.ewi.utwente.nl/assignments/completed/master/reports/thesis_ooms_06_07.pdf

[3] 3rd Generation Partnership Project, www.3GPP.org

[4] International Telecommunication Union, www.itu.int

[5] de Laat, C., Gross, G., Gommans, L., Vollbrecht, J., Spence, D., "Generic AAA Architecture", IETF RFC 2903, August 2000

[6] Madjid Nakhjiri and Mahsa Nkhjiri, "AAA and Network Security for Mobile Access", Wiley, 2005.

[7] Vollbrecht, J., Calhoun, P., Farrell, S., Gommans, L., Gross, G., de Bruijn, B., de Laat, C., Holdrege, M., and D. Spence, "AAA Authorization Framework", IETF RFC 2904, August 2000

[8] Liberty Alliance, www.liberty.org

[9] Fried, J., Sword, D., "Making IMS Work: Current Realities, Challenges And Successes", Empirix Inc., May 1, 2006, http://www.bcr.com/architecture/ip_networking/making_ims_work_200605011199.htm

[10] Perry, D. E., Elliott Sim, S., , Easterbook, S., "Case studies for Software Engineers", Proceedings of ICSE 2004 tutorial, 2004.

[11] Whittle J., Krüger, I., H., "A Methodology for Scenario-Based Requirements Capture", Proceedings of the ICSE 2004 Workshop on Scenarios and State Machines (SCESM), 2004, http://www-cse.ucsd.edu/~ikrueger/publications/WhittleKrueger_SCESM04_final.pdf

[12] Calhoun, P., Loughney, J., Guttman, E., Zorn, G., Arkko, J., "Diameter Base Protocol", IETF RFC 3588, September 2003

[13] Lal Das, M., Saxena, A., Gulati, V., P., "A Dynamic ID-based Remote User Authentication Scheme", Consumer Electronics, IEEE Transactions on Volume 50, Issue 2, May 2004

[14] Calhoun, P., Zorn, G., Spence, D., Mitton, D., "Diameter Network Access Server Application", IETF RFC 4005, August 2005

[15] Calhoun, P., Johansson, T., Perkins, C., Hiller, T., McCann, P., "Diameter Mobile IPv4 Application", IETF RFC 4004, August 2005

[16] Neuman, C., Yu, T., Hartman, S., Raeburn, K., "The Kerberos Network Authentication Service (V5)", IETF RFC 4120, July 2005

[17] 3GPP specification, "3GPP Technical Specification Group Services and System Aspects; IP Multimedia Subsystem (IMS); Stage 2 (Release 8)", TS 23.228 V8.1.0, June 2007, http://www.3gpp.org/ftp/Specs/html-info/23228.htm