Inter-domain Authentication and Authorization Mechanisms for Roaming SIP Users

Dorgham Sisalem, Jiri Kuthan
Fraunhofer Institute for Open Communication Systems (FhG Fokus)
Kaiserin-Augusta-Allee 31, 10589 Berlin, Germany

Abstract: To enable users to utilize the services of various providers of multimedia services based on the session initiation protocol (SIP), some kind of interaction is required between the foreign provider and the home provider of the users. Such interaction is required for example to allow a user to utilize services provided by a foreign service provider while the user is on travel. In this paper we describe two possible approaches for exchanging authentication, authorization and accounting (AAA) information between foreign and home providers, namely: SIP dependent and independent inter-domain AAA communication. In the SIP dependent scenario, SIP is used as the communication protocol between the interacting providers and for carrying any information that needs to be exchanged between the providers. With the SIP independent scenario a special AAA protocol is used between the domains for exchanging AAA related information. Both approaches will be described in terms of message sequences that would be exchanged and will be analyzed in terms of their efficiency, flexibility and security. The here described scenarios present an overview of various efforts currently being followed in the standardization groups and are based on standardized protocols. Our contribution is to provide the details of the currently discussed concepts and compare between them.

Introduction

The recent advances in the telecommunication market in the form of high speed access networks and integration of messaging, VoIP, location-based services and other multimedia services based on the session initiation protocol (SIP) 0 as well as the availability of low-cost wireless access technologies, is leading to the emergence of a new breed of network and service providers. Those providers not only differ in their used access technology and provided services but also in their business models and structures. Such providers can range from large providers such as the current telecom providers offering multiple-services and covering large geographical areas down to small providers offering certain services such as conferencing or messaging only or covering small geographical areas such as a coffee shop or a shopping mall. For such providers to offer their services in a profitable manner they need to have as large user base as possible. Having to establish a contractual relation with each user before offering him a service is usually a long and costly procedure.

Sisalem D. and Kuthan J. (2004).
Inter-domain Authentication and Authorization Mechanisms for Roaming SIP Users.
In *Proceedings of the 3rd International Workshop on Wireless Information Systems*, pages 89-99
DOI: 10.5220/0002668300890099

The experience gained from the enormously successful pre-paid and call-by-call charging models suggest that users appreciate the liberty of being allowed to choose between different providers without having to establish a contractual relation with those providers in advance. Transferring such a model would mean that a user could use a VoIP service from a provider A to reach any location in Europe whereas he would use a provider B to reach the USA. For such a model to function efficiently in an all-IP environment, the service providers need to be able to establish trust relations with their users and naturally be able to charge them. Identifying and authenticating a user directly is in general a tedious task that is bugged by scalability and security problems that have hindered until now the wide usage of public key infrastructures for example. Therefore the common approach propagated in the all-IP environment is to identify a home provider that has a contractual relation with the user and ask the home provider to authenticate and authorize the user. Thereby the trust problem is reduced to establishing trust relations between providers.

While in the current networking environment, a home provider of a user is usually represented by a large telecom provider, in an all-IP environment, any trustworthy entity such as an application provider, a banking entity or a credit-card provider that is capable of authenticating the user and maintaining his usage profile can act as a home provider. To provide a service to a visiting user some kind of interaction between the foreign provider and the home provider is required. In this paper we will be looking at two distinctive approaches for exchanging authentication, authorization and accounting (AAA) information between foreign and home providers, namely: SIP dependent and independent inter-domain AAA communication. In the SIP dependent scenario, see Sec. 2, SIP is used as the communication protocol between the interacting providers and is used for carrying any information that needs to be exchanged between the providers. With the SIP independent scenario, see Sec. 3, a special AAA protocol such as RADIUS 0 or DIAMETER 0 is used between the domains for exchanging AAA related information. Both approaches will be described in terms of message sequences that would be exchanged and will be analyzed in terms of their efficiency, flexibility and security. In Sec. 4 a general comparison between the two scenarios is presented.

1 General Overview of SIP

The most important SIP operation is that of inviting new participants to a call. To achieve this functionality we can distinguish different SIP entities:

- **Proxy:** A proxy server receives a request and then forwards it towards the current location of the callee -either directly to the callee or to another server that might be better informed about the actual location of the callee.
- **Redirect:** A redirect server receives a request and informs the caller about the next hop server. The caller then contacts the next hop server directly.
- **User Agent:** A logical entity in the terminal equipment that is responsible for generating and terminating SIP requests.
- **Registrar:** To assist SIP entities in locating the requested communication partners SIP supports a further server type called register server. The register

server is mainly thought to be a database containing locations as well as user preferences as indicated by the user agents.

-

In SIP, a user is identified through a SIP URI in the form of user@domain. This address can be resolved to a SIP proxy that is responsible for the user's domain. To identify the actual location of the user in terms of an IP address, the user needs to register his IP address at the SIP registrar responsible for his domain. Thereby when inviting a user, the caller sends his invitation to the SIP proxy responsible for the user's domain, which checks in the registrar's database the location of the user and forwards the invitation to the callee. The callee can either accept or reject the invitation. The session initiation is then finalized by having the caller acknowledging the reception of the callee's answer. During this message exchange, the caller and callee exchange the addresses at which they would like to receive the media and what kind of media they can accept. After finishing the session establishment, the end systems can exchange data directly without the involvement of the SIP proxy.

For authenticating a user SIP uses the digest authentication mechanisms, which is based on a challenge/reply approach. In our discussion we will be assuming that a roaming user is supposed to contact a local SIP proxy in the foreign network. This is especially needed when the local proxies offer some kind of local services such as emergency calls or are used to enforce local policies, as is the case with 3GPP IMS networks 0.

2 SIP Dependent Inter-Domain AAA Communication

In this scenario the SIP signalling messages are used for initiating and controlling the communication sessions as well as negotiating AAA aspects among the providers. Here we assume that both the caller and callee are present in foreign networks. The approach depicted in Figure 1 is very close to the one used in the IP multimedia system (IMS) of 3GPP0, for more information.

In our presentation we assume that the INVITE message always includes the SDP part, which could also have been carried in a following message. We also assume that the session establishment consists of the exchange of an INVITE, 200 OK and ACK messages. In the 3GPP model in which QoS reservation is integrated into the session establishment, a row of other messages needs to be exchanged as well, for instance 183 Session Progress, PRACK followed by 200 OK for acknowledging the reception of the 183 message, an UPDATE message followed by 200 OK indicating the status of the QoS reservation and only then the final 200 OK and ACK for the session establishment0. Note however, that those further messages are not involved in the authorization procedure and hence their inclusion would only complicate the scenario without added benefit.

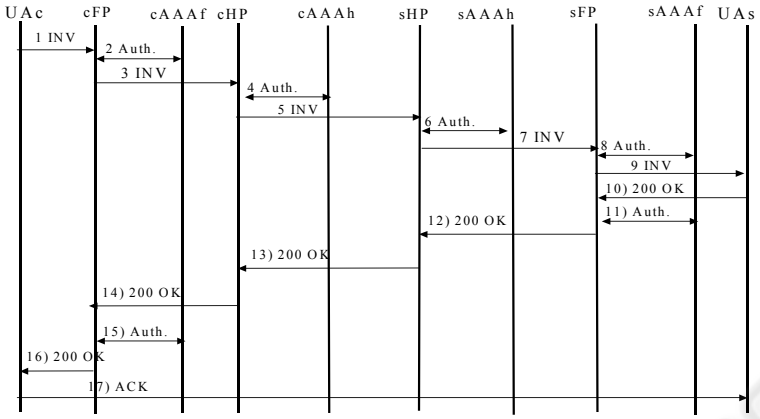

Figure 1 SIP dependent inter-domain AAA exchange

Abbreviations:

- UAc: user agent client (caller)
- cFP SIP proxy in the foreign domain in which the client is present
- cAAAf: AAA server in the foreign domain in which the client is present
- cHP: home proxy of the client
- cAAAh: AAA server in the home domain of the client
- sHP: Home proxy of the user agent server
- sAAAh: AAA server in the home domain of the server
- sFP: SIP proxy in the foreign domain in which the server is present
- sAAAf: AAA server in the foreign domain in which the server is present
- UAs: user agent server (callee)

The authorization is realized in this scenario in the following steps:

1. The caller issues an INVITE towards the local proxy in the foreign domain (cFP). The address of this proxy is configured while assigning the host with an IP address using DHCP for example 0. The INVITE message indicates the characteristics of the call in the SDP part (which codecs and media type and whether QoS reservation is required)
2. The cFP consults with a local AAA server to check local policies regarding initiating calls and whether this user is eligible for initiating calls with the given parameters (is the required bandwidth is reasonable for instance). If not, the call is rejected or the session description is modified by deleting codecs or media styles the user is not allowed to use. To make sure that all subsequent requests pass this proxy a Record-Route entry can be added to the SIP message.

3. After receiving a positive answer the INVITE is forwarded to the home proxy of the caller. To make sure that all subsequent requests pass this proxy a Record-Route entry can be added to the SIP message. The home proxy of the user can be discovered in one of two ways:
   - Based on the domain name part of the FROM header in the INVITE
   - In 3GPP, see 0, the route is decided during an initial registration phase in which the domain part of the Request-URI is used to identify a proxy (ICSCF) in the home domain. At the home domain, a serving proxy (SCSCF) is identified and added to a header called the P-Service-Route 0 header, which is then mirrored in the reply. The routes included in the P-Service-Route header are then used to guide the proxies of where to direct the SIP messages.
4. The home proxy checks with its AAA server whether the user is eligible for initiating a session with the characteristics indicated in the INVITE. If not the call is rejected or the session description is modified by deleting codes or media styles the user is not allowed to use.
5. The INVITE is forwarded to the home proxy of the callee.
6. The home proxy of the callee might check with its local AAA server (sAAAh) whether the user is allowed to receive calls with the indicated characteristics. If not the call is rejected or the session description is modified by deleting codecs or media styles the user is not allowed to use. The home proxy also checks with its registration database the current location of the user and adds a Record-Route entry as well.
7. The message is forwarded to the SIP proxy in the foreign domain in which the user is currently present. This proxy can be discovered in the following manner:
   - The user might indicate in his REGISTER message the domain in which he is currently in.
   - With the 3GPP approach a special header is added to the REGISTER message, the PATH header 0, in which, traversed proxies during the registration step indicate whether they should be contacted for incoming requests to the user.
8. The sFP might need to check with the local AAA server (sAAAf) to check local policies and whether the user is eligible for receiving calls. If not the call is rejected or the session description is modified by deleting codecs or media styles the user is not allowed to use.
9. The INVITE is forwarded to the callee.
10. The callee replies with a 200 OK including its media and QoS preferences to the sFP
11. The sFP has now the entire session data (IP addresses and port numbers as well as exchanged media for both communicating end systems) and can authorize the session. That is the AAA server creates an entry for this session describing the involved end systems and the compression style, bandwidth and media the communicating end systems are allowed to use.
12. Based on the VIA list in the SIP header the 200 OK is forwarded to the sHP
13. Based on the VIA list in the SIP header the 200 OK is forwarded to the cHP
14. Based on the VIA list in the SIP header the 200 OK is forwarded to the cFP

15. The cFP can now authorize the session based on the complete knowledge of the communication parameters (IP addresses and port numbers as well as chosen media). That is the AAA server creates an entry for this session describing the involved end systems and the compression style, bandwidth and media the communicating end systems are allowed to use.
16. 200 OK message is forwarded to the caller
17. The session is established by sending an ACK message to the callee. The ACK will traverse proxies traversed by the INVITE due to the Record-Route entries added during the invitation part.

From the description of this authorization interaction it is clear that the inter-domain exchange of AAA information is implicit in nature. That is, the foreign provider considers a non-negative reply that has passed the home provider as an indication that the user is allowed to establish a session in the form indicated in the signalling messages. On the other side, the home provider considers a request originating from a foreign provider as authorized by that provider.

2.1 Evaluation of the SIP Dependent Inter-Domain AAA Communication

- **Complexity:** Each provider can use his own proprietary AAA servers. All inter-domain communication is then realized based on the standardized SIP messages. That is, no separate inter-domain AAA communication is required. This reduces the complexity of the provider's infrastructure. However, this increases the complexity of the SIP signalling itself. Authentication and authorization information are of utmost importance as they might reveal information about the monetary status of a user and his allowed services. Any tampering of that information might allow an interceptor to establish communication sessions on the costs of other users. Due to this the SIP messages need to be specially protected to prevent such misuse, which increases the complexity of using SIP.
- **Performance:** Application signalling needs always to traverse the home provider even if it would have been possible to signal some session directly to the called party without going through the home provider's network first. This would in general mean longer round trip delays. Further, updates to the used resources, i.e., accounting information, must be also sent to the home provider. This can be achieved either by using a special protocol between the foreign and home network or by carrying the information in the SIP messages. Using a special protocol would diminish the advantage of having only one protocol to worry about, i.e., SIP. On the other hand carrying accounting information with SIP, means that SIP message are used to carry information that is only of interest to certain proxies. In this scenario, the end systems could generate SIP requests (the INFO message would be a candidate), the foreign proxy would retrieve accounting data from the local AAA server and add the information to the INFO and forward it to the home proxy of the user. The home proxy retrieves the accounting data, deletes them from the message and informs its local AAA server about the received accounting data. This naturally raises the question of how the providers would act if the end systems did not generate these INFO messages. On the one hand this increases the complexity of SIP proxies and reduces the performance as it increases the size of the SIP messages. Another option is for the home provider to subscribe to the accounting

state of the foreign provider. With this option, the foreign provider would generate an event describing the current accounting state of the user after each change of this state. This incurs further message exchange to establish the subscription, updates it and deletes it at the end of the communication session in addition to the notifications themselves. Note that this approach is already being standardized for the usage of SIP in 3GPP 0with the goal of providing home networks the possibility of terminating sessions of their subscribers currently located in a foreign network.

- **Convenience:** Convenience here indicates the convenience to the home provider. With this scenario, the home providers can check the eligibility of the user's requests during each action and directly take actions by rejecting a request for example or changing the session description. This gives the home provider a better view of and control on the user's actions.
- **Security:** For the foreign network to accept the AAA data generated by the home network and vice-versa some kind of security association between the two networks needs to be established. This might still need some integration of the providers with a PKI infrastructure or some security broker to dynamically establish such an association, especially when dealing with a large number of providers.
- **Flexibility:** With this scenario, an authorative provider, i.e., a provider that can authenticate the user and which maintains the user's profile and authorization information, must be reachable through SIP. That is, this authorative provider must have a SIP infrastructure consisting of proxies and registrars beside the AAA servers and the users would have the name of the provider as part of their SIP address. This increases the hurdles for an independent provider such as a banking entity to act as an authorative provider.

3 SIP Independent Inter-Domain AAA Communication

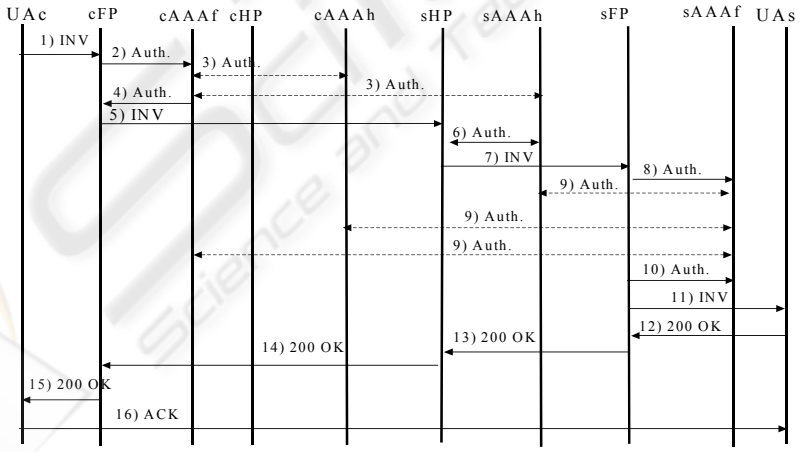

Figure 2 SIP independent inter-domain AAA exchange with SIP dependent intra-domain authorization

In this scenario the AAA data is exchanged using special protocols between AAA entities. This approach utilizes the AAA infrastructure defined by the IETF, see 0 and

0 and is also deployed by the Mobile-IP protocol, see 0. That is during the application signalling phase, an entity in the foreign network would ask the home AAA server of the user through a dedicated AAA protocol for authentication and authorization data of the user.

As depicted in Figure 2 the message flow is rather different than in the SIP dependent scenario:

1. The session starts with the user issuing an INVITE message towards the local proxy (cFP).
2. The cFP asks its local AAA server whether the user is allowed to continue the call. Note that this step is only relevant if the foreign provider wants to charge the user for some service or needs to authenticate him.
3. In this step the local AAA server consults another AAA server to authorize the call. Here we can distinguish two cases:
   a. **Call paid by the caller:** The local AAA server contacts the home AAA server of the caller (cAAAh) to authenticate the user and authorize the call.
   b. **Call paid by callee:** The local AAA server contacts the home AAA server of the callee (sAAAh) to authorize the call.

   This choice can be implemented in the form of a policy entry driven for example by the identity of the caller and/or callee. Further in some cases both steps might be needed. This is the case, when the foreign network wants to authenticate the caller and still charge the callee for the call. Note that the cAAAh and sAAAh do not necessarily need to have a relation with the home SIP providers (cHP and sHP). Actually any entity, which is reachable over the used AAA protocol and is capable of authenticating and authorizing the user and can be trusted by the asking provider, can take the role of the AAAh server. However, SIP messages usually only carry the SIP identity of the caller and callee in the form of the FROM, To and R-URI header. Therefore, to instruct the cAAAf server to contact a special AAA server a new SIP header needs to be added to the SIP messages indicating the name of this AAA server. Thereby the cAAAf would contact the AAA server indicated in the SIP messages and ask for authentication and authorization information of the user. The user might be represented with his SIP name (FROM header) or yet another entry to be added to the SIP messages.
4. The result of the inter-domain AAA exchange as well as the local AAA actions is sent to the proxy (cFP).
5. The INVITE is forwarded to the home proxy of the callee.
6. The home proxy of the callee (sHP) checks with its local AAA server whether the callee is allowed to receive calls with the signalled content. Note that this step might be skipped if the sAAAh was already contacted in step 3.
7. The sHP checks in its registration database the current location of the user and forwards the INVITE either directly to that location or to the foreign proxy serving the current domain of the user (sFP).
8. The sFP checks with its local AAA server (sAAAf) whether the callee is eligible for receiving calls with the parameters signalled in the INVITE message.
9. In case the incoming call incurs certain costs in the foreign network in which the callee is currently located the local AAA server (sAAAf) needs to contact some other AAA server to authorize the call. Depending on who is paying for the call the sAAAf can contact one of three possible AAA servers:

a. **Call paid by caller:** In this case the sAAAf would contact the cAAAh and check the eligibility of the caller to make such a call.
b. **Call paid by foreign provider:** In this model, the caller would pay the foreign network of the UAs indirectly. In this case the sAAAf would contact the cAAAf to check whether that foreign provider of the UAc is willing to pay for the call that originated from its domain. The foreign provider of the caller would then add the costs for the resources in the foreign network of the UAs to the costs incurred in its own network to the bill of the caller.
c. **Calls paid by callee:** In this case the sAAAf contacts the AAA server of the callee to check the eligibility of the callee to receive this call.

The choice of which AAA server to contact can be made twofold

- **Local policy:** Based on some local policies such as all calls coming to foreign users are to be charged by those users or that based on the identity of the users a certain AAA server is to be contacted.
- **Authorization tokens:** An authorization token can be used to indicate that the call was authorized by a AAA server and that this AAA server should be contacted for any further questions with regard to the eligibility of this call. Thereby, such a token might include some information characterizing the call such as the call-ID and FROM and TO headers signed by the public key of the authorizing AAA server. Further, the token needs to contain information readable by any proxy indicating the name of the authorizing proxy so as to be contacted if needed. Thereby, in step 3 the cAAAf, cAAAh or the sAAAh might generate such a token that would then be handed to the SIP proxy, which would include it in the forwarded SIP INVITE. The proxy needing to authorize a call would check this token, contact the AAA server indicated in it and send it the session information encrypted in the token as well as the list of resources requested by the call. The contacted AAA server would then reply on whether the user is allowed to utilize those resources, see 0 for a variation of this approach.

10. The final authorization decision is now made based on the local policy of the sAAAh as well as the exchanged AAA information with another AAA server as described in step 9.
11. The INVITE is forwarded to the user agent server.
12. The UAs answers with an OK 200 sent to the sFP.
13. The sFP forwards the 200 OK to the sHP.
14. The sHP forwards the 200 OK to the cFP.
15. The cFP forwards the 200 OK to the user agent client.
16. The client finishes the session establishment by sending an ACK message.

Unless the home proxy of the callee (sHP) wants to be on the path of all future requests by adding a Record-Route entry in the first INVITE message, requests can now be exchanged directly between the foreign proxies, i.e., form cFP to sFP.

3.1 Evaluation of SIP Independent Inter-Domain AAA Communication

- **Complexity:** While different application level protocols might provide varying degrees of secure communication a well-designed AAA protocol must have these

features. This might allow for simpler application protocols that trust that the providers are using a secure AAA protocol for exchanging user data. That is, in this case, the security requirements on the SIP messages can be reduced. However, the providers need to support yet another protocol and standardized components.

- **Performance:** Only the AAA data need to be exchanged between the foreign and home network whereas the application signalling data can be exchanged directly between the caller and callee. This reduces the load on the home provider's proxies and reduces the signalling delay. Accounting data can also be exchanged over the AAA infrastructure without having the need for a separate protocol or the need for integrating the data with the application signalling protocols. In case the SIP home providers need to be on the signalling path in order to provide the users with some services, the SIP independent AAA exchange would be wasteful as inter-domain communication between the home and foreign providers would be triggered twice: once for the SIP signalling and once for the AAA exchange.
- **Convenience:** For the home provider to be able to control each action of the users the SIP signalling messages need to traverse the home provider which would diminish the performance benefits that could be obtained by having the SIP messages exchanged directly between the communicating end systems. Another option would be to use the AAA infrastructure to inform the home provider about the actions of the user. This would, however, increase the load on the AAA infrastructure.
- **Flexibility:** Defining the business relations between the different providers might be simplified. As described in Figure 2 the specification of who is to pay for which call can be signalled during the call establishment without requiring pre-defined and static roaming agreements. Also, the definition of a home provider is broadened here. Any entity providing a AAA server can act as an authorative home provider without necessarily having to offer a SIP infrastructure.

4 General Performance Comparison between SIP Dependant and Independent Inter-Domain AAA Communication

In terms of delay if we assumed that the round trip delay between two components inside the same domain can be set to 0.5 T unit, with T as some amount of time, and the round trip delay between two components in different domains is set to T then the SIP independent scenario described in Figure 2 would consume 7.5 T units to finish the session establishment. The SIP dependent scenario requires between 6 and 7 T units depending on whether all the AAA servers possibly involved are contacted and whether the cFP is contacted before forwarding the INVITE.

In general, we can also add that both schemes show a considerable level of complexity. Thereby, when actually introducing the one or the other, the implementers need to consider the exact communication scenario and base their choice of which approach to use on that scenario.

5 Summary

In this paper we described two different approaches for authenticating and authorizing roaming users wanting to use SIP-based services. In the description of the scenarios we used simplified signalling scenarios to reduce the complexity of the description.

On the one hand, this allowed us to better describe the scenarios in an understandable manner and provided us with a qualitative impression of the advantages and disadvantages of each approach. However, on the other hand this prevented us from achieving a completely accurate comparison in terms of number of used messages and message sizes. This can only be realized after a detailed definition of the communication scenario and AAA protocols and infrastructure used. Nevertheless, this brief overview already gives a clear picture of the pros and cons of each approach. Probably the most valuable result obtained here is that all scenarios have their pros and cons and which one to use can only be decided based on the usage scenario, the supported services and the current infrastructure of the provider.

References

1. J. Rosenberg, H. Schulzrinne, G. Camarillo, A. Johnston, J. Peterson, R. Spark, M. Handley, E. Schooler, “Session Initiation Protocol”, RFC3261
2. 3GPP Technical Specification 3GPP TS 33.102 V3.6.0: "Technical Specification Group Services and System Aspects; 3G Security; Security Architecture (Release 1999)", 3rd Generation Partnership Project, November 2000
3. Pat R. Calhoun, et al.; ”Diameter Base Protocol”, RFC 3358, September 2003
4. Rigney, C., Willens, S., Rubens, A. and W. Simpson, "Remote Authentication Dial In User Service (RADIUS)", RFC 2865, June 2000.
5. H. Schulzrinne, “Dynamic Host Configuration Protocol (DHCP-for-IPv4) Option for Session Initiation Protocol (SIP) Servers” RFC 3361, August 2002
6. D. Willis, B. Hoeneisen, “Session Initiation Protocol (SIP) Extension Header Field for Service Route Discovery During Registration “, RFC 3608, October 2003
7. 3GPP Technical Specification 3GPP TS 24.228 " Technical Specification Group Core Network; Signalling flows for the IP multimedia call control based on SIP and SDP", 3GPP, 2003
8. J. Vollbrecht, P. Calhoun, S. Farrell, L. Gommans, G. Gross, B. de Bruijn, C. de Laat, M. Holdrege, D. Spence: AAA Authorization Framework; IETF, RFC 2904, August 2000.
9. J. Vollbrecht, P. Calhoun, S. Farrell, L. Gommans, G. Gross, B. de Bruijn, C. de Laat, M. Holdrege, D. Spence: AAA Authorization Application Examples; IETF, RFC 2905, August 2000.
10. S. Glass, T. Miller, S. Jacobs, C. Perkins, “Mobile IP Authentication, Authorization, and Accounting Requirements”, IETF, RFC 2977, October 2000
11. W. Marshall, F. Andreasen, D. Evans, “Private Session Initiation Protocol (SIP) Extensions for Media Authorization”, RFC 3312, January 2003
12. Sinnreich, Rawlins, Gross, Thomas, "QoS and AAA Usage with SIP based IP communication", Internet Draft, Internet Engineering Task Force, October 2001
13. Camarillo, et al., “Integration of Resource Management and SIP”, RFC 3312, October 2002