Internet Engineering Task Force
INTERNET-DRAFT
draft-ietf-sipping-aaa-req-02.ps

SIP WG
J. Loughney, G. Camarillo
Nokia, Ericsson

February 5, 2003
Expires: August, 2003

Authentication, Authorization and Accounting Requirements for the Session Initiation Protocol

Status of this Memo

Copyright Notice

Abstract

As SIP services are deployed on the Internet, there is a need for authentication, authorization and accounting of SIP sessions. This document sets out the basic requirements for this work.

Contents

1 Introduction **2**
1.1 Terminology and Acronyms 3
1.2 Requirements Language 3

2 Requirements **3**
2.1 Common Requirements 3
2.1.1 Communication within the same domain 3
2.1.2 Communication between different domains 4
2.1.3 Discovery 4
2.1.4 Ability to Integrate Different Networks, Services and Users 4
2.1.5 Updating SIP Server Entries 4
2.1.6 Call Setup Times 4
2.1.7 Security 4
2.2 Authentication Requirements 4
2.2.1 Authentication Based on SIP Requests 4
2.2.2 Flexible Authentication of SIP requests 4
2.3 Authorization Requirements 5

2.3.1 Ability to Authorize SIP Requests 5
2.3.2 Information transfer 5
2.3.3 Distribution of Profiles 5
2.3.4 User De-authorization 5
2.4 Accounting Requirements 5
2.4.1 Separation of Accounting Information 5
2.4.2 Accounting Information Related to Session Progression 5
2.4.3 Accounting Information Not Related to Session Progression 6
2.4.4 Support for One-Time and Session-based Accounting Records 6
2.4.5 SIP Session Changes 6
2.4.6 Support for Accounting on Different Media Components 6
2.4.7 Support for Stateful and Stateless Accounting 6
2.4.8 Configuration of Accounting Generation Parameters 6
2.4.9 Support for Arbitrary Correlation IDs 6
2.4.10 Support for Real-time and Non-Realtime Accounting 6
2.4.11 Flexible Interface 6

3 Scenarios **7**
3.1 WLAN Roaming Using Third Party Service Providers 7
3.2 Simple 3GPP Example 8

4 Security Considerations **8**

5 Acknowledgements **8**

6 Authors' Addresses **9**

1 Introduction

The AAA working group is chartered to work on authentication, authorization and accounting solutions for the Internet. This work consists of a base protocol, applications, end-to-end security application and a general architecture for providing these services [3]. The AAA working group has specified applicability of AAA-based solutions for a number of protocols (e.g., AAA requirements for Mobile IP [4]).

SIP is a signalling protocol for creating, modifying and terminating different types sessions such as Internet phone calls, multimedia distribution and multimedia conferences [1]. SIP sessions have needs for session authentication, authorization and accounting. In order to perform AAA, SIP entities need to access AAA information (e.g., check if the password provided by a user is correct or store accounting records related to a particular session). Rather than collocating a database with AAA information with every SIP entity in a network, it is desirable to have a common logical AAA server accessible by all the SIP entities. SIP entities use a SIP-AAA interface to access this AAA server. This document outlines some requirements on this SIP-AAA interface between SIP entities and AAA servers. This document is intended as a generic document for SIP AAA requirements. It does not intend to develop a charging and/or billing mechanism for SIP.

One possible use of this document would be to create a basic AAA application for SIP needs.

The protocol used in the SIP-AAA interface could be any protocol that meets the requirements outlined by this document. Possible candidates, among others, are Diameter and XML-based protocols following the web-services model.

1.1 Terminology and Acronyms

AAA: Authentication, Authorization and Accounting

Accounting: In this draft, accounting is meant in a broad sense, not simply charging or billing.

Home AAA Server: Server where user with which the user maintains an account relationship.

Online Accounting: Also known as real-time accounting. Downloading some kind of credit into the access device, and deducting from that credit as usage accumulates.

Offline Accounting: Also known as non-realtime accounting. Transferring records to a home accounting server, for later billing and settlement, without doing any accounting-related control or feedback for the services rendered.

SIP: Session Initiation Protocol

UAC: User Agent Client

UAS: User Agent Server

Proxies: Proxies are nodes which forward requests and responses as well as make policy decisions.

1.2 Requirements Language

In this document, the key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" are to be interpreted as described in RFC 2119 [2].

2 Requirements

In this section, we list the requirements. It is assumed that different situations, deployment scenarios will affect which requirements are needed. It is not intended that all requirements need to be supported. Section 2.1 lists general requirements, Section 2.2 lists requirements related to authentication, Section 2.3 lists requirements related to authorization and Section 2.4 lists requirements related to accounting.

2.1 Common Requirements

This section outlines general requirements on the SIP-AAA interface.

2.1.1 Communication within the same domain

The SIP-AAA interface MUST support communications between a SIP entity and a AAA server that belong to the same domain.

2.1.2 Communication between different domains

The SIP-AAA interface MUST support communications between a SIP entity in one domain and a AAA server in another domain.

2.1.3 Discovery

With the information contained in the SIP messages, the SIP-AAA interface MUST be able to deduct the particular AAA server that has to be queried.

2.1.4 Ability to Integrate Different Networks, Services and Users

The basic AAA architecture MUST be access independent. Service providers have to be able to provide AAA services for SIP, irrespective of access method or technology.

2.1.5 Updating SIP Server Entries

When required, the SIP-AAA interface MUST allow the AAA server to update the information about a user that a SIP entity has.

2.1.6 Call Setup Times

AAA SHOULD not unduly burden call setup times where appropriate. It may be reasonable to support some delay during registration, but delay during sessions (especially real-time) are problematic.

2.1.7 Security

AAA data MUST be able to be securely transported. The endpoints MUST be authenticated before data is sent. The endpoints MAY be authorized to access certain types of AAA data.

2.2 Authentication Requirements

This section outlines requirements on the SIP-AAA interface related to authentication.

2.2.1 Authentication Based on SIP Requests

The home AAA server MUST be able to authenticate a user based on any SIP request, except CANCEL.

> CANCEL is a hop-by-hop request that can be generated by proxies that do not have the user's credentials.

2.2.2 Flexible Authentication of SIP requests

The scheme supported for the authentication between the SIP servers and the AAA infrastructure MUST be flexible enough to accommodate a variety of authentication mechanisms. In particular, the SIP-AAA interface MUST be able to accommodate all the authentication mechanisms mandated by the SIP specs.

2.3 Authorization Requirements

This section outlines requirements on the SIP-AAA interface related to authorization.

2.3.1 Ability to Authorize SIP Requests

The SIP-AAA interface MUST allow AAA servers to authorize any SIP request, except CANCEL.

> CANCEL is a hop-by-hop request that can be generated by proxies. SIP servers receiving a CANCEL do not challenge it, as they would do with an end-to-end request. Instead, they check that the entity sending the CANCEL is the same as the one that generated the request being canceled.

2.3.2 Information transfer

The SIP-AAA interface MUST allow transfering a wide range or set of information to be used to make an authorization decision.

2.3.3 Distribution of Profiles

The SIP-AAA interface MUST allow a AAA server that is making an authorization decision to deliver the user profile to the SIP entity. Note that the user profile may provide further information about the authorization decision to the SIP entity. For instance, a SIP proxy receives an INVITE from user A addressed to user B. The SIP proxy queries a AAA server and gets the following answer: user A is authorized to call user B as long as the requests are routed through a particular SIP proxy server C. In this case, the SIP proxy needs to use SIP loose routing techniques to forward the INVITE so that it traverses SIP proxy C before reaching user B.

2.3.4 User De-authorization

The SIP-AAA interface MUST allow the AAA server to inform a SIP entity when a particular user is no longer authorized to perform a particular task, even if it is an ongoing task.

2.4 Accounting Requirements

This section outlines requirements on the SIP-AAA interface related to accounting. Accounting is more than simple charging. Accounting may be a simple list of services accessed, servers accessed, duration of session, etc. Charging for SIP sessions can be extremely complex and requires some additional study. It is not the intent of this section to focus on charging.

2.4.1 Separation of Accounting Information

AAA accounting messages MUST be able to separate ”session duration” information from other information generated via additional services (e.g., 3-way calling, etc.) Separating accounting information makes it possible to charge different parties for different aspects of the session.

2.4.2 Accounting Information Related to Session Progression

There MUST be support in the SIP-AAA interface for accounting transfers where the information contained in the accounting data has a direct bearing on the establishment, progression and termination of a session.

2.4.3 Accounting Information Not Related to Session Progression

There MUST be support in the SIP-AAA interface for accounting transfers where the information contained in the accounting data does NOT have a direct bearing on the establishment, progression and termination of a session.

2.4.4 Support for One-Time and Session-based Accounting Records

The SIP-AAA interface MUST allow SIP servers to provide relevant accounting information for billing and inter-network settlement purpose to the AAA servers. Both one-time event accounting records and session based (START, INTERIM, STOP records) accounting MUST be supported.

2.4.5 SIP Session Changes

Accounting messages MUST be able to reflect changes in the SIP session that affects the charging of SIP session.

2.4.6 Support for Accounting on Different Media Components

The SIP-AAA interface MUST support accounting per media component (e.g., voice and video). The SIP-AAA interface MUST enable different parties to be charged per media component.

2.4.7 Support for Stateful and Stateless Accounting

Stateful and stateless accounting (also referred to as cumulative and non-cumulative accounting) MUST be supported by the SIP-AAA interface.

2.4.8 Configuration of Accounting Generation Parameters

The SIP-AAA interface MUST allow AAA servers to communicate parameters for accounting generation.

2.4.9 Support for Arbitrary Correlation IDs

Some networks need to be able to relate the accounting to some aspect of the session. Therefore, the SIP-AAA interface MUST support arbitrary correlation IDs.

2.4.10 Support for Real-time and Non-Realtime Accounting

Real-time and Non-Realtime Accounting MUST be supported by the SIP-AAA Interface. Real-time accounting allows implementing credit-based charging, where an application checks the end user's account for coverage for the requested service event charge prior to execution of that service event (authorization).

2.4.11 Flexible Interface

The scheme supported for the accounting between the SIP servers and the AAA infrastructure MUST be flexible enough to accommodate a variety of accounting mechanisms.

3 Scenarios

This section outlines some possible scenarios for SIP and AAA interaction. These are purely illustrative examples, and do not impose any requirements.

Figure 1 shows the typical call flow between a SIP proxy that communicates to a AAA server that performs authentication and authorization. All the examples are based on this flow.

```
SIP            SIP            AAA
UAC           Proxy         Server

 |              |              |
 |---METHOD---->|              |
 |              |--Is it OK?-->|
 |              |              |
 |              |<-----OK------|
 |              |              |
 |              |              |
```

Figure 1: Call flow over the SIP-AAA interface

The SIP proxy receives a request with certain credentials. The SIP UAC that generated the request may have included the credentials after having been challenged by the proxy using a 407 (Proxy Authentication Required) response. The SIP proxy sends a request to the AAA server asking if it is OK to provide a particular service for this request. The service may be simply routing forward the request or may consist of a more complex service. The AAA server checks that the credentials are correct (authentication), and checks the user profile. The user profile indicates that it is OK to provide the service, and responds to the SIP proxy. The SIP proxy provides the service requested by the SIP UAC.

3.1 WLAN Roaming Using Third Party Service Providers

User A wants to establish a voice session over the Internet with user B. User A wants its SIP signalling to be routed through SIP proxy C, because it provides a call log service (i.e., SIP proxy C sends an email to user A once a month with the duration of all the calls made during the month.)

User A accesses the Internet using a WLAN access outside his home domain. User A, user B, SIP proxy C and the home AAA server of user A are all in different domains.

SIP proxy C challenges the initial INVITE from user A with a 407 (Proxy Authentication Required) response, and user A reissues the INVITE including his credentials. SIP proxy C consults user's A home AAA server, which confirms that the credentials belong to user A and that SIP proxy C can go ahead and provide its service for that call. SIP proxy C routes the INVITE forward towards user B and sends an accounting message to the AAA server, which will be used later to charge user A for the service provided by SIP proxy C.

```
                        SIP               AAA
      User A          Proxy C           Server          User B

        |                |                 |                |
        |----INVITE----->|                 |                |
        |                |                 |                |
        |<-----407-------|                 |                |
        |                |                 |                |
        |------ACK------>|                 |                |
        |                |                 |                |
        |----INVITE----->|                 |                |
        |                |---Is this OK?-->|                |
        |                |                 |                |
        |                |<------OK--------|                |
        |                |                 |                |
        |                |---------INVITE------------------>|
        |                |                 |                |
        |                |-Accounting msg->|                |
        |                |                 |                |
```

Figure 2: WLAN roaming user

3.2 Simple 3GPP Example

User A is not in his home domain, but it still uses SIP proxy C, which is in user's A home domain, as the outbound proxy for an INVITE. SIP proxy C consults the home AAA server, which indicates that requests from user A have to be routed through SIP proxy D. SIP proxy C uses SIP loose routing so that the INVITE traverses D before reaching its destination. SIP proxy D will provide call log service for user A.

The example in figure 3 illustrates roughly how a SIP based 3GPP network works.

4 Security Considerations

This document is informational in nature, so it does not directly affect the security of the Internet. However, security is a basic requirement of this work.

5 Acknowledgements

The authors would like to thank the participants of the SIP interim meeting, May 2002 for their comments. The authors would also thank Harri Hakala, Mary Barns, Pete McCann and Henry Sinnreich for their comments.

The authors would like to thank the authors of the "AAA Requirements for IP Telephony/Multimedia" draft, which some of the information in this document is based on.

```
                       SIP                    AAA         SIP
     User A          Proxy C                Server     Proxy D

       |                |                      |           |
       |----INVITE----->|                      |           |
       |                |                      |           |
       |<-----407-------|                      |           |
       |                |                      |           |
       |------ACK------>|                      |           |
       |                |                      |           |
       |----INVITE----->|                      |           |
       |                |------Is this OK?---->|           |
       |                |                      |           |
       |                |<-OK if routed thru D-|           |
       |                |                      |           |
       |                |---------INVITE------------------>|
       |                |                      |           |
```

Figure 3: 3GPP example

6 Authors' Addresses

John Loughney
Nokia Research Center
Itmerenkatu 11-13
00180 Helsinki
Finland
electronic mail: john.Loughney@nokia.com

Gonzalo Camarillo
Ericsson
Advanced Signalling Research Lab.
FIN-02420 Jorvas
Finland
electronic mail: Gonzalo.Camarillo@ericsson.com

Normative References

[1] J. Rosenberg, H. Schulzrinne, G. Camarillo, A. R. Johnston, J. Peterson, R. Sparks, M. Handley, and E. Schooler, “SIP: session initiation protocol,” RFC 3261, Internet Engineering Task Force, June 2002.

[2] S. Bradner, “Key words for use in rfcs to indicate requirement levels,” RFC 2119, Internet Engineering Task Force, Mar. 1997.

Informative References

[3] P. Calhoun *et al.*, “AAA problem statements,” internet draft, Internet Engineering Task Force, Nov. 2000. Work in progress.

[4] S. Glass, T. Hiller, S. Jacobs, and C. E. Perkins, “Mobile IP authentication, authorization, and accounting requirements,” RFC 2977, Internet Engineering Task Force, Oct. 2000.

Full Copyright Statement