Network Working Group
Request for Comments: 3665
BCP: 75
Category: Best Current Practice

A. Johnston
MCI
S. Donovan
R. Sparks
C. Cunningham
dynamicsoft
K. Summers
Sonus

December 2003

Session Initiation Protocol (SIP) Basic Call Flow Examples

Status of this Memo

Copyright Notice

Abstract

This document gives examples of Session Initiation Protocol (SIP) call flows. Elements in these call flows include SIP User Agents and Clients, SIP Proxy and Redirect Servers. Scenarios include SIP Registration and SIP session establishment. Call flow diagrams and message details are shown.

Table of Contents

1. Overview

The call flows shown in this document were developed in the design of a SIP IP communications network. They represent an example minimum set of functionality.

It is the hope of the authors that this document will be useful for SIP implementers, designers, and protocol researchers alike and will help further the goal of a standard implementation of RFC 3261 [1]. These flows represent carefully checked and working group reviewed scenarios of the most basic examples as a companion to the specifications.

These call flows are based on the current version 2.0 of SIP in RFC 3261 [1] with SDP usage described in RFC 3264 [2]. Other RFCs also comprise the SIP standard but are not used in this set of basic call flows.

Call flow examples of SIP interworking with the PSTN through gateways are contained in a companion document, RFC 3666 [5].

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in BCP 14, RFC 2119 [4].

1.1. General Assumptions

A number of architecture, network, and protocol assumptions underlie the call flows in this document. Note that these assumptions are not requirements. They are outlined in this section so that they may be taken into consideration and to aid in the understanding of the call flow examples.

The authentication of SIP User Agents in these example call flows is performed using HTTP Digest as defined in [1] and [3].

Some Proxy Servers in these call flows insert Record-Route headers into requests to ensure that they are in the signaling path for future message exchanges.

These flows show TCP, TLS, and UDP for transport. See the discussion in RFC 3261 for details on the transport issues for SIP.

1.2. Legend for Message Flows

Dashed lines (---) represent signaling messages that are mandatory to the call scenario. These messages can be SIP or PSTN signaling. The arrow indicates the direction of message flow.

Double dashed lines (===) represent media paths between network elements.

Messages with parentheses around their name represent optional messages.

Messages are identified in the Figures as F1, F2, etc. This references the message details in the list that follows the Figure. Comments in the message details are shown in the following form:

```
 /* Comments. */
```

1.3. SIP Protocol Assumptions

This document does not prescribe the flows precisely as they are shown, but rather the flows illustrate the principles for best practice. They are best practices usages (orderings, syntax, selection of features for the purpose, handling of error) of SIP methods, headers and parameters. IMPORTANT: The exact flows here must not be copied as is by an implementer due to specific incorrect characteristics that were introduced into the document for convenience and are listed below. To sum up, the basic flows represent well-reviewed examples of SIP usage, which are best common practice according to IETF consensus.

For simplicity in reading and editing the document, there are a number of differences between some of the examples and actual SIP messages. For example, the HTTP Digest responses are not actual MD5 encodings. Call-IDs are often repeated, and CSeq counts often begin at 1. Header fields are usually shown in the same order. Usually only the minimum required header field set is shown, others that would normally be present such as Accept, Supported, Allow, etc are not shown.

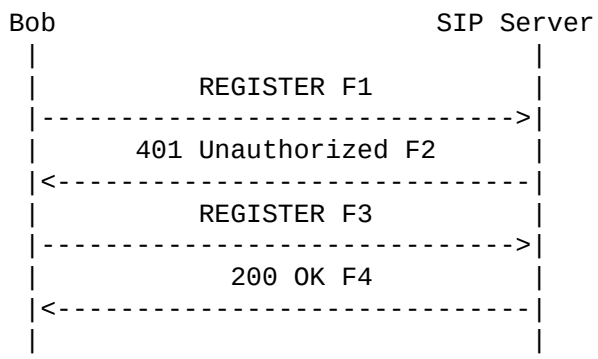
Actors:

Element	Display Name	URI	IP Address
User Agent	Alice	alice@atlanta.example.com	192.0.2.101
User Agent	Bob	bob@biloxi.example.com	192.0.2.201
User Agent		bob@chicago.example.com	192.0.2.100
Proxy Server		ss1.atlanta.example.com	192.0.2.111
Proxy/Registrar		ss2.biloxi.example.com	192.0.2.222
Proxy Server		ss3.chicago.example.com	192.0.2.233
ALG		alg1.atlanta.example.com	192.0.2.128

2. SIP Registration

Registration binds a particular device Contact URI with a SIP user Address of Record (AOR).

2.1. Successful New Registration



Bob sends a SIP REGISTER request to the SIP server. The request includes the user's contact list. This flow shows the use of HTTP Digest for authentication using TLS transport. TLS transport is used due to the lack of integrity protection in HTTP Digest and the danger of registration hijacking without it, as described in RFC 3261 [1]. The SIP server provides a challenge to Bob. Bob enters her/his valid user ID and password. Bob's SIP client encrypts the user information according to the challenge issued by the SIP server and sends the response to the SIP server. The SIP server validates the user's credentials. It registers the user in its contact database and returns a response (200 OK) to Bob's SIP client. The response includes the user's current contact list in Contact headers. The format of the authentication shown is HTTP digest. It is assumed that Bob has not previously registered with this Server.

Message Details

F1 REGISTER Bob -> SIP Server

```
REGISTER sips:ss2.biloxi.example.com SIP/2.0
Via: SIP/2.0/TLS client.biloxi.example.com:5061;branch=z9hG4bKnashds7
Max-Forwards: 70
From: Bob <sips:bob@biloxi.example.com>;tag=a73kszlfl
To: Bob <sips:bob@biloxi.example.com>
Call-ID: 1j9FpLxk3uxtm8tn@biloxi.example.com
CSeq: 1 REGISTER
Contact: <sips:bob@client.biloxi.example.com>
Content-Length: 0
```

DOCKET ALARM

Explore Litigation Insights

Docket Alarm provides insights to develop a more informed litigation strategy and the peace of mind of knowing you're on top of things.

Real-Time Litigation Alerts

Keep your litigation team up-to-date with **real-time alerts** and advanced team management tools built for the enterprise, all while greatly reducing PACER spend.

Our comprehensive service means we can handle Federal, State, and Administrative courts across the country.

Advanced Docket Research

With over 230 million records, Docket Alarm's cloud-native docket research platform finds what other services can't. Coverage includes Federal, State, plus PTAB, TTAB, ITC and NLRB decisions, all in one place.

Identify arguments that have been successful in the past with full text, pinpoint searching. Link to case law cited within any court document via Fastcase.

Analytics At Your Fingertips

Learn what happened the last time a particular judge, opposing counsel or company faced cases similar to yours.

Advanced out-of-the-box PTAB and TTAB analytics are always at your fingertips.

API

Docket Alarm offers a powerful API (application programming interface) to developers that want to integrate case filings into their apps.

LAW FIRMS
Build custom dashboards for your attorneys and clients with live data direct from the court.

Automate many repetitive legal tasks like conflict checks, document management, and marketing.

FINANCIAL INSTITUTIONS
Litigation and bankruptcy checks for companies and debtors.

E-DISCOVERY AND LEGAL VENDORS
Sync your system to PACER to automate legal marketing.