3GPP TSG CN Plenary Meeting #17 **NP-020393**
4th - 6th September 2002. Biarritz, France.

Source:	**Chairs, SIP, SIPPING, and SIMPLE Working Groups of the Internet Engineering Task Force**
Title:	**Liaison Statement on Interoperability Issues and SIP in IMS**
Agenda item:	**5.2**
Document for:	**INFORMATION**

From: Rohan Mahy [rohan@cisco.com]
Sent: Sunday, September 01, 2002 2:20 PM
To: stephen.hayes@am1.ericsson.se; statements@ietf.org
Cc: mankin@isi.edu; sob@harvard.edu; dean.willis@softarmor.com; rohan@cisco.com; brian.rosen@marconi.com; jo@ipdialog.com; jon.peterson@neustar.biz; 'Robert Sparks'
Subject: Liaison Statement on Interoperability Issues and SIP in IMS

From: Chairs, SIP, SIPPING, and SIMPLE Working Groups of the Internet Engineering Task Force
Cc: Area Directors, Transport Area, Internet Engineering Steering Group
To: CN and SA Working Groups of the Third-Generation Partnership Program
Subject: Liaison Statement on Interoperability Issues and SIP in IMS

I. Introduction

The IETF is made up of working groups, such as the Session Initiation Protocol (SIP) Working Group, and these are supervised by the Internet Engineering Steering Group, or IESG, whose goals include maintaining technical quality and assuring that its work is consistent with the "big picture" of Internet principles and architecture. The IETF also has the Internet Architecture Board, or IAB, ensuring the big picture is clear.

The IESG's Area Director for SIP, and the IESG as a whole have given repeated guidance to the SIP Working Group in the process of development and approval of the consensus standards such as RFC 3261, during which several points have been raised that we believe are related to the usage of SIP in the Internet Multimedia Subsystem (IMS) specifications being developed in 3GPP. Our goal is to communicate these points at a technical level, from the consensus of our approved standards, as the Working Group chairs, to you as counterpart technical Working Group chairs. We wish to convey introductory points here, points about interoperability in section 2, and specific issues about the IETF SIP standards in section 3.

The key guidance is:

a) Internet standards are intended to have broad applicability for all aspects of the Internet, including private networks that use IP, whether or not connected to the public network. Developing "profiles"--subsets of or exceptions to these standards, whether for use on public or private networks, is dangerous because of the very high probability that such profiles will be incompatible with those deployed on the Internet as a whole, and we have learned that networks which are disconnected today somehow become connected tomorrow. Thus inter-operability remains a critical issue, even for currently disconnected networks.

b) Any implementation of a protocol claimed or named to be an Internet protocol, such as SIP, should be greatly consistent with both the specification and the practice of that protocol on the Internet. If an implementation doesn't interoperate, and/or does not operate (if suitably configured) in general Internet environments, it is actually a separate protocol and should not be advertised or named the same as an implementation of an Internet protocol.

We believe that 3GPP chose to use SIP and other Internet protocols in the IMS specification not only as a matter of expedient reuse, but because of advantages such as interoperability, open specification, and widespread deployment offered by these protocols. Further, we believe that 3GPP's choice was influenced by the expectation that these Internet advantages would lead to benefits such as reduced systems cost, access to a wide variety of applications being developed around the Internet, and the consequent ability to develop and offer new value-added applications to wireless subscribers and generate new revenue for wireless operators. We support this choice and rationale, and welcome 3GPP as a collaborator in making the best possible use of our protocols. To that end, we welcome 3GPP input on requirements for the unique aspects of their environment, in the further
development of SIP and other Internet protocols, and look forward to collaborating with 3GPP to facilitate developing the best understanding for all about how best to configure SIP and other Internet protocols for interoperability between the IM subsystem and the Internet.

II. Interoperability Issues

Careful review of published IMS specifications, by knowledgeable individuals who participate in both 3GPP and IETF, has raised certain concerns relating to interoperability (both in terms of a and b) between IMS and the Internet. The Chairs of the IETF SIP and SIPPING Working Groups offer this liaison statement as guidance and suggestions to 3GPP, in hopes of assuring effective interoperability. We realize that some of these concerns stem from recent enhancements to the SIP protocol, and cannot be immediately rectified in the IMS specifications, whereas other concerns may be more readily addressable. We encourage 3GPP to address these concerns to the extent possible in IMS Release 5, and to address them and any underlying issues before the finalization of IMS Release 6. We will assist wherever reasonably possible, and welcome further involvement with 3GPP to resolve these concerns.

In general, we would like 3GPP to consider two interopability goals:

1) While operator and business policy configurations (which are not matters of IETF concern) may prevent such behavior, the IMS specification itself should not prevent the possibility that an IMS user can access SIP services on the Internet, or establish SIP sessions with users on the Internet. This should be possible without requiring that some sort of application-level-gateway to modify the IMS protocols. In most cases, we expect that an IMS user should be able to access Internet applications even if there is no explicit support in IMS for that application. This implies that IMS users have access to complete SIP implementations including security capabilities.

2) The SIP specification (RFC 3261) and the other related IETF standards allow for building strong and secure Internet applications. An IMS operator should be able to buy an off-the-shelf, IETF standard, commercial SIP system that implements the RFCs related to SIP, and which also has support for IMS-specific capabilites, plug it in, use configuration options to set up policies, and make it work in IMS systems. Configuration and local policies would establish
what local authentication, authorization, AAA, reporting, SIP P-headers, and other options are used that might not be widely implemented in the Internet--or indeed are not in the case of P-headers.

Vendors building an IMS system should not need to build two completely separate products to address IMS and SIP in the Internet. The key point here is that there should be little or no difference other than the configuration choices conceptually in an implementation used in IMS and one used outside IMS. This would be an ideal interoperability goal, and well suited to the IETF's orientation of standardizing what is implemented and available to the operator or user of the equipment (e.g. minimum mandatory to implement strong security), not what is used or how it is used.

III. Specific Concerns on SIP in IMS Release 5

The following discusses some of our technical concerns with IMS. It should be noted that this is by no means an exhaustive list of issues. It is intended primarily to introduce the types of behaviors that concern us and the probable impact of these behaviors on interoperability. However, where specific issues are illustrated, we request specific consideration of these concerns by 3GPP.

There are three general classes of issues that we have identified:

1. IMS Call State Control Function (CSCF) nodes send messages that the SIP RFCs reserve to User Agents without implementing the functions required for User Agents. There is some 3GPP view that this is justified by viewing the CSCF as a "back to back user agent" with the User Agent, but it is not done correctly, because the CSCF must be implemented in all ways as User Agent in order to be serve as a B2BUA in this manner.

2. IMS CSCF nodes modify headers in ways explicitly prohibited to proxies by the SIP RFCs, again without implementing associated UA behavior.

3. IMS CSCF nodes modify bodies in messages which is not permitted to proxies by SIP RFCs, again without implementing the associated UA behavior.

A number of participants in the SIP working group, including the chairs authoring this liaison statement, have identified specific concerns with the IMS Release 5 specifications as we understand them. Some of these have been discussed in the context of SIP or SIPPING chartered work. We do not propose solutions here, but we invite consideration of these concerns, with the goal of 3GPP achieving a better alignment to the IETF's SIP RFCs after discussion in 3GPP and in the SIP and SIPPING mailing lists over some period. IETF will provide any support and assistance that will help.

1) The P-CSCF may send a BYE on behalf of the UA, generally because the P-CSCF has been notified by the radio layer that the UA has lost contact. Of course, the P-CSCF doesn't have the credentials to provide authentication of the BYE, so many UAs will consider this to be a forged message. This also renders 3GPP UAs vulnerable to denial of service attacks using forged BYEs.

2) The P-CSCF strips away Route, Record-Route, Via, Path, and Service-Route headers before passing messages on to the UA. It then reinserts them messages in the other direction, and may also strip out Route headers inserted by the UA. This breaks end-to-end protection using S/MIME and prevents the UA from

accessing external services using loose routing. It also prevents the UA from knowing about any proxies that may have piggybacked on its registration using the Path mechanism, which is a serious violation of the openness principle and leaves 3GPP users registering with external servers subject to certain man-in-the-middle attacks affecting REGISTER messages without any way to detect those attacks.

3) The CSCF may edit SDP sent from or to the UA in order to force the selection of codecs considered favorable to the operator. This has the side effect of breaking end-to-end protection of the SDP using S/MIME. It also precludes interoperating with external elements when both the IMS UA and the external UA share only a common codec not supported by the P-CSCF.

4) The S-CSCF MAY (we believe this is still being discussed in 3GPP) obfuscate the To: and From: fields in messages. This appear to be based on a particular interpretation of privacy regulation in certain European domains. It has the side effect of breaking end-to-end protection with S/MIME and breaking external services using the To: and From: fields, such as the most common forms of caller-ID used with SIP today.

5) The P-CSCF filters messages from the UA to assure that only an identity known to the P-CSCF is presented by the UA. This may interact with the preceding characteristic. This appears to be required to accommodate the authorization model of 3GPP, which authenticates only REGISTER transactions and uses them to establish a security association between a UA and the P-CSCF. The side effect is that a 3GPP user may use only the operator-provided identity and may not be able to effectively use third-party services that provide other identities unless those services provide identity transformation with a back-to-back user agent.

6) The I-CSCF (or THIG) may encrypt Via and Route information when acting in topology-hiding mode. This was allowed for in earlier SIP specifications, but the use has been deprecated for a variety of reasons. The exact impact on interoperability remains unknown.

7) Some CSCF elements and AS may manipulate message bodies. Manipulating message bodies in a proxy is forbidden in RFC 3261 because it breaks end-to-end protection using S/MIME. These elements do not appear to implement all of the UA behavior that would enable them to preserve end-to-end protections.

As stated above, this statement does not recommend a timeframe for aligning on the issues decribed above, but they are important. One way to ensure better aligment going forward is in a general recommendation.
The SIP Working Group chairs suggest that the implementers of systems for IMS should consider doing interoperability testing of their implementations against other SIP implementations. The SIPit interoperability events are organized explicitly for this purpose, and we intend to use these events to support the documentation of interoperability of features required for advancing SIP and related RFCs from "Proposed Standard" to "Draft Standard" status in the IETF. Your participation in such testing would be helpful to the whole SIP community.

IV. Contacts:

Dean Willis, dean.willis@softarmor.com, for SIP Working Group Chairs

Rohan Mahy, rmahy@cisco.com, for other SIP-related WGs' Chairs
Allison Mankin, mankin@isi.edu, for the IESG