Internet Engineering Task Force (IETF)
Request for Comments: 5947
Category: Informational
ISSN: 2070-1721

J. Elwell
Siemens Enterprise Communications
H. Kaplan
Acme Packet

September 2010

Requirements for Multiple Address of Record (AOR) Reachability Information in the Session Initiation Protocol (SIP)

Abstract

This document states requirements for a standardized SIP registration mechanism for multiple addresses of record (AORs), the mechanism being suitable for deployment by SIP service providers on a large scale in support of small to medium sized Private Branch Exchanges (PBXs). The requirements are for a solution that can, as a minimum, support AORs based on E.164 numbers.

Status of This Memo

This document is not an Internet Standards Track specification; it is published for informational purposes.

This document is a product of the Internet Engineering Task Force (IETF). It represents the consensus of the IETF community. It has received public review and has been approved for publication by the Internet Engineering Steering Group (IESG). Not all documents approved by the IESG are a candidate for any level of Internet Standard; see Section 2 of RFC 5741.

Information about the current status of this document, any errata, and how to provide feedback on it may be obtained at http://www.rfc-editor.org/info/rfc5947.

Table of Contents

1. Introduction 3
2. Terminology 3
3. Problem Statement 4
   3.1. Issues with the REGISTER Transaction 5
        3.1.1. Mishandling by SIP-Aware Middleboxes 5
        3.1.2. REGISTER Response Growth 6
        3.1.3. Illegal "Wildcard" Syntax 6
   3.2. Issues with Routing Inbound Requests to the SIP-PBX 6
        3.2.1. Loss of Target Information 6
        3.2.2. Inconsistent Placement of Target URI Information in Inbound Requests 6
        3.2.3. Request-URI Misrouting 7
   3.3. Policy-Related Issues 7
        3.3.1. Authorization Policy Mismatches 7
        3.3.2. PAI or PPI URI Mismatches 7
4. Requirements 8
5. Desirables 10
6. Non-Requirements 11
7. Security considerations 11
8. Acknowledgements 12
9. References 12
   9.1. Normative References 12
   9.2. Informative References 12

1. Introduction

The Session Initiation Protocol (SIP) [RFC3261], together with its extensions, supports multiple means of obtaining the connection information necessary to deliver out-of-dialog SIP requests to their intended targets. When a SIP proxy needs to send a request to a target address of record (AOR) within its domain, it can use a location service to obtain the registered Contact Universal Resource Identifiers (URIs), together with any associated path information [RFC3327], and build a route set to reach each target user agent (UA). The SIP REGISTER method can be used to register Contact URIs and path information. SIP-outbound [RFC5626] enhances this mechanism to cater to UAs behind Network Address Translators (NATs) and firewalls. When an entity needs to send a request to a target for which it is not authoritative, the entity can follow [RFC3263] procedures for using the Domain Name System (DNS) to obtain the next-hop connection information.

In practice, many small- and medium-sized businesses use a SIP Private Branch Exchange (SIP-PBX) that is authoritative for tens or hundreds of SIP AORs. This SIP-PBX acts as a registrar/proxy for these AORs for users hosted by the SIP-PBX. A SIP Service Provider (SSP) provides SIP peering/trunking capability to the SIP-PBX. The SIP-PBX needs to be reachable from the SSP so that the SSP can handle inbound out-of-dialog SIP requests targeted at these AORs, routing these requests to the SIP-PBX for onward delivery to registered UAs.

Experience has shown that existing mechanisms are not always sufficient to support SIP-PBXs for small/medium businesses. In particular, RFC 3263 procedures are generally inappropriate, except for some larger SIP-PBXs. In current deployments, mechanisms for the dynamic provision of reachability information based on the SIP REGISTER method are commonly used. However, these mechanisms vary in detail, leading to interoperability issues between SIP-PBXs and SSPs, and the need for equipment to support different variants. A more detailed statement of the problem is given in Section 3.

This document states requirements for a standardized SIP registration mechanism for multiple AORs, the mechanism being suitable for deployment by SSPs on a large scale in support of small- to medium-sized SIP-PBXs. The requirements are for a solution that can, as a minimum, support AORs based on E.164 numbers.

2. Terminology

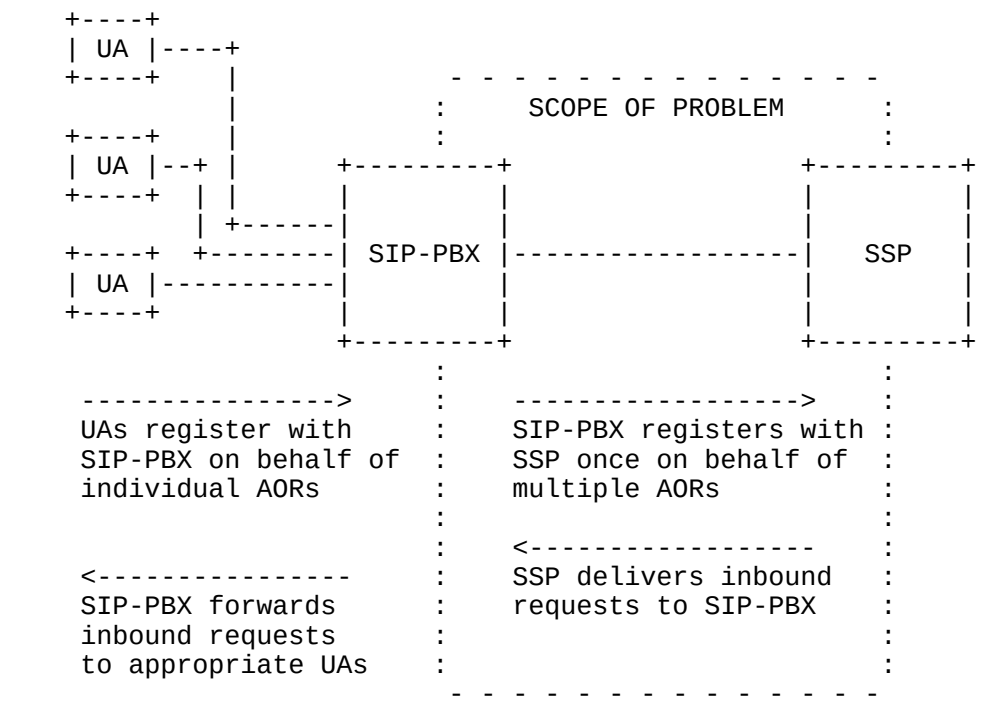
The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in [RFC2119].

The terms address of record (AOR), proxy, REGISTER, registrar, request, response, and user agent (UA) are to be interpreted as described in [RFC3261].

3. Problem Statement

A number of other standards organizations have addressed the issue of a SIP-PBX registering with its SSP, notably ETSI [ETSI_TS_182025] and 3rd Generation Partnership Project (3GPP) [3GPP.24.229]. Also, various SSPs have produced proprietary specifications for use with their own offerings. The reader is encouraged to review the documents produced by those organizations.

A short summary of the general concept is as follows. The figure below illustrates the scope of the problem.



In virtually all models, the SIP-PBX generates a SIP REGISTER request using a mutually agreed-upon SIP AOR -- typically based on the SIP-PBX's main attendant-/reception-desk number. The AOR is often in the domain of the SSP, and both the To and From URIs used for the REGISTER request identify that AOR. In all respects, it appears on

the wire as a "normal" SIP REGISTER request, as if from a typical user's UA. However, it generally implicitly registers other AORs associated with the SIP-PBX.

For both 3GPP and ETSI mechanisms, the 200 OK response to the REGISTER request, sent after a successful authentication challenge, contains a P-Associated-URI (PAU) [RFC3455] header field listing the other SIP URIs or TEL URIs (i.e., phone numbers) of the SIP-PBX, which are implicitly registered AORs. The registered reachability information from the REGISTER request will be used to reach not only the single explicitly registered AOR but also each of the implicitly registered AORs. In order to reduce the number of PAU entries, a "wildcard" syntax model is defined [3GPP.23.003], which uses a regular expression syntax in the user field of the URI to express multiple AORs in a compressed manner.

For routing requests for any of the explicitly or implicitly registered AORs from the SSP to the SIP-PBX, the Request-URI is typically replaced with the registered Contact URI. In the case of 3GPP and ETSI, the SSP has the option of using loose routing instead, and inserting the registered Contact URI as a loose route Route header field value, while leaving the Request-URI alone. This decision is made based upon manually provisioned information in the registrar's database (i.e., the Home Subscriber Server (HSS)).

3.1. Issues with the REGISTER Transaction

3.1.1. Mishandling by SIP-Aware Middleboxes

None of the currently available mechanisms indicate that the REGISTER request or response is any different from a "normal" REGISTER request or response. This has caused issues when SIP-aware middleboxes between the SIP-PBX and the registrar serve both SIP-PBXs and normal UAs yet need to apply different policies to the two cases.

Furthermore, some middleboxes expect the registrar to follow normal [RFC3261] procedures of Request-URI replacement with the registered Contact URI for routing subsequent requests to the SIP-PBX. If the registrar adopts a different practice for requests to SIP-PBXs, this can cause the middlebox to fail to route such requests correctly, because there is no indication that the registration was any different.

Lastly, lack of an indication of implicit registration makes troubleshooting more difficult because the on-the-wire messages are indistinguishable from "normal" registrations. Note that even the

existence of a PAU header field in the response does not indicate that implicit registration for a SIP-PBX has occurred, since the PAU header field is also used for normal UAs with multiple identities.

3.1.2. REGISTER Response Growth

If a SIP-PBX represents many AORs, the PAU list in the response can grow the SIP message size beyond the limits for UDP.

3.1.3. Illegal "Wildcard" Syntax

The current syntax for "wildcarded" PAUs is illegal for TEL URIs, based on the ABNF rules for TEL URIs in [RFC3966].

3.2. Issues with Routing Inbound Requests to the SIP-PBX

3.2.1. Loss of Target Information

If the proxy-registrar follows [RFC3261] for registration resolution of requests targeted at one of the SIP-PBX's AORs, and thus replaces the Request-URI with the registered Contact URI, it is not clear which AOR is the intended target of the request. The To URI, for example, may not contain the intended target AOR if the request was forwarded/retargeted prior to reaching the proxy-registrar. Some middleboxes between the registrar and SIP-PBX will overwrite the Request-URI specifically to try to fix this issue. In some cases, a P-Called-Party-ID header field [RFC3455] will contain the intended target AOR; and in some cases, the History-Info header field [RFC4244] will contain it. The SIP-PBX needs to know where to look to find the required information and, in the case of History-Info, needs to identify the particular element containing the required information.

3.2.2. Inconsistent Placement of Target URI Information in Inbound Requests

Even when all information needed by the SIP-PBX is provided, in some deployments, inbound SIP requests from the SSP have the registered SIP-PBX Contact URI in the Request-URI, whereas in other deployments inbound SIP requests have the intended target SIP-PBX user (AOR) in the Request-URI and the Contact URI in the Route header field. There are other variants, too. Interoperability problems arise when a SIP-PBX designed or configured for one variant attempts to interwork with an SSP designed or configured for another variant.

3.2.3. Request-URI Misrouting

Although many SIP-PBXs support registration with an SSP, they do not consider themselves authoritative for the explicitly or implicitly registered AORs if the domain portion still identifies the SSP's domain. They expect the domain portion to be their own IP Address, Fully Qualified Domain Name (FQDN), or domain. Currently, middleboxes have to fix that issue.

3.3. Policy-Related Issues

The following are largely policy matters for the SSP, but it should be noted the policies described below will not work in some situations. A mechanism for solving the SIP-PBX registration problem will not solve these policy issues directly, although when specifying the mechanism, the opportunity can be taken to highlight the impact of such policies.

3.3.1. Authorization Policy Mismatches

Many SSPs perform a first-order level of authorization for requests from the SIP-PBX by checking the URI in the From, P-Asserted-Identity (PAI), or P-Preferred-Identity (PPI) [RFC3325] header field for one matching either an explicitly or implicitly registered AOR for the same Contact URI and/or Layer-3 IP Address. However, some SIP-PBXs change the Contact URI they use for non-REGISTER requests to be different from the one they explicitly registered. For example, they change the user portion of the Contact URI, or even the host portion. This is particularly true for a SIP-PBX operating as a proxy and forwarding the Contact URI from the UA behind the SIP-PBX (the SIP-PBX typically being identified in a Record-Route header field), rather than acting as a Back-to-Back User Agent (B2BUA) and substituting its own Contact URI. This can cause an SSP to fail to find an AOR corresponding to the Contact URI for non-REGISTER requests, resulting in the SSP rejecting such requests or asserting its own PAI value, rather than asserting a value based on received header fields.

3.3.2. PAI or PPI URI Mismatches

Some SSPs expect the PAI or PPI URI in SIP requests received from the SIP-PBX to match one of the explicitly or implicitly registered AORs, whereas some SIP-PBXs generate the URIs using their local IP Address, hostname, or domain name. Some SSPs expect the PAI or PPI URI in SIP requests received from the SIP-PBX to be the explicitly registered

AOR only, as it is the main billing number, instead of the implicitly registered AOR of the calling party. In either case, this can result in the SSP rejecting requests with values that do not match, or asserting its own PAI value.

Again, these are policy matters for the SSP, but drawbacks should be noted. For example, rejection of requests can rule out requests from sources beyond the SIP-PBX (e.g., calls forwarded by the SIP-PBX), unless the SIP-PBX changes the PAI or PPI URI to a value acceptable to the SSP (in which case it will no longer identify the calling user). If the SSP changes the PAI or PPI URI, again the request will fail to identify the calling user.

4. Requirements

The following are requirements of the mechanism.

REQ1: The mechanism MUST allow a SIP-PBX to enter into a trunking arrangement with an SSP whereby the two parties have agreed on a set of telephone numbers assigned to the SIP-PBX.

REQ2: The mechanism MUST allow a set of assigned telephone numbers to comprise E.164 numbers, which can be in contiguous ranges, discrete, or in any combination of the two.

REQ3: The mechanism MUST allow a SIP-PBX to register reachability information with its SSP, in order to enable the SSP to route to the SIP-PBX inbound requests targeted at assigned telephone numbers.

REQ4: The mechanism MUST allow UAs attached to a SIP-PBX to register with the SIP-PBX for AORs based on assigned telephone numbers, in order to receive requests targeted at those telephone numbers, without needing to involve the SSP in the registration process.

REQ5: The mechanism MUST allow a SIP-PBX to handle requests originating at its own UAs and targeted at its assigned telephone numbers, without routing those requests to the SSP.

REQ6: The mechanism MUST allow a SIP-PBX to receive requests to its assigned telephone numbers originating outside the SIP-PBX and arriving via the SSP, so that the SIP-PBX can route those requests onwards to its UAs, as it would for internal requests to those telephone numbers.

REQ7: The mechanism MUST provide a means whereby a SIP-PBX knows at which of its assigned telephone numbers an inbound request from its SSP is targeted.

REQ8: The mechanism MUST provide a means of avoiding problems due to one side using the mechanism and the other side not.

In other words, the mechanism is required to avoid the situation where one side believes it is using the mechanism and the other side believes it is not, e.g., the SIP-PBX believes it is performing the registration of multiple telephone numbers, but the SSP believes a single AOR is being registered.

REQ9: The mechanism MUST observe SIP backwards compatibility principles.

In other words, the mechanism is required to provide a graceful means of recovery or fall-back if either side does not support the mechanism. For example, this might involve the use of an option tag.

REQ10: The mechanism MUST work in the presence of a sequence of intermediate SIP entities on the SIP-PBX-to-SSP interface (i.e., between the SIP-PBX and the SSP's domain proxy), where those intermediate SIP entities indicated during registration a need to be on the path of inbound requests to the SIP-PBX.

These intermediate SIP entities can be edge proxies, session border controllers, etc.

REQ11: The mechanism MUST work when a SIP-PBX obtains its IP address dynamically.

REQ12: The mechanism MUST work without requiring the SIP-PBX to have a domain name or the ability to publish its domain name in the DNS.

REQ13: For a given SIP-PBX and its SSP, there MUST be no impact on other domains, which are expected to be able to use normal RFC 3263 procedures to route requests, including requests needing to be routed via the SSP in order to reach the SIP-PBX.

REQ14: The mechanism MUST be able to operate over a transport that provides end-to-end integrity protection and confidentiality between the SIP-PBX and the SSP, e.g., using Transport Layer Security (TLS) as specified in [RFC3261].

REQ15: The mechanism MUST support authentication of the SIP-PBX by the SSP and vice versa, e.g., using SIP digest authentication plus TLS server authentication as specified in [RFC3261].

REQ16: The mechanism MUST allow the SIP-PBX to provide its UAs with public or temporary Globally Routable UA URIs (GRUUs) [RFC5627].

REQ17: The mechanism MUST work over any existing transport specified for SIP, including UDP.

REQ18: Documentation MUST give guidance or warnings about how authorization policies may be affected by the mechanism, to address the problems described in Section 3.3.

REQ19: The mechanism MUST be extensible to allow a set of assigned telephone numbers to comprise local numbers as specified in [RFC3966], which can be in contiguous ranges, discrete, or in any combination of the two.

REQ20: The mechanism MUST be extensible to allow a set of arbitrarily assigned SIP URI’s as specified in [RFC3261], as opposed to just telephone numbers, without requiring a complete change of mechanism as compared to that used for telephone numbers.

5. Desirables

The following are desirable properties of the mechanism.

In addition to the desirables below, the general aim is to require only relatively modest changes to a substantial population of existing SSP and SIP-PBX implementations, in order to encourage a fast market adoption of the standardized mechanism. Ease of market adoption is paramount here. Many SIP-PBXs and SSPs have implemented mechanisms based on the REGISTER method, and the need for substantial changes to those implementations will discourage convergence on a single standard in the foreseeable future.

DES1: The mechanism SHOULD allow an SSP to exploit its mechanisms for providing SIP service to normal UAs in order to provide a SIP trunking service to SIP-PBXs.

DES2: The mechanism SHOULD scale to SIP-PBXs of several thousand assigned telephone numbers.

This will probably preclude any mechanism involving a separate REGISTER transaction per assigned telephone number.

In practice, the mechanism is more likely to be used on SIP-PBXs with up to a few hundred telephone numbers, but it is impossible to give a precise limit, and hence the desire to be able to support several thousand.

DES3: The mechanism SHOULD scale to support several thousand SIP-PBXs on a single SSP.

6. Non-Requirements

The means by which a third domain can route a request to the SSP for onward delivery to the SIP-PBX is outside the scope of this work. This is related to REQ13, which requires normal routing based on RFC 3263 be used.

Provisioning is outside the scope of this work. In particular, an SSP will need to assign a set of telephone numbers to a SIP-PBX, and a SIP-PBX will need to be aware of the set of assigned numbers and allocate those numbers to its users. Automated means for a SIP-PBX to obtain, from its SSP, the set of assigned telephone numbers is considered to be a provisioning topic.

7. Security considerations

The security of signaling between the SIP-PBX and the SSP is important. Some of the requirements above already address this.

In particular, it is important that an entity acting as a SIP-PBX cannot register with an SSP and receive inbound requests to which it is not entitled. The SSP is assumed to have procedures for ensuring that a SIP-PBX is entitled to use a set of E.164 telephone numbers prior to entering into agreement with that SIP-PBX for using those telephone numbers with this mechanism. Furthermore, by authenticating the SIP-PBX when it provides reachability information, the SSP can be sure that it delivers inbound requests only to the correct destination.

8. Acknowledgements

The contents of the document have been compiled from extensive discussions within the MARTINI WG, the individuals concerned being too numerous to mention.

9. References

9.1. Normative References

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.

[RFC3261] Rosenberg, J., Schulzrinne, H., Camarillo, G., Johnston, A., Peterson, J., Sparks, R., Handley, M., and E. Schooler, "SIP: Session Initiation Protocol", RFC 3261, June 2002.

[RFC3263] Rosenberg, J. and H. Schulzrinne, "Session Initiation Protocol (SIP): Locating SIP Servers", RFC 3263, June 2002.

9.2. Informative References

[RFC3325] Jennings, C., Peterson, J., and M. Watson, "Private Extensions to the Session Initiation Protocol (SIP) for Asserted Identity within Trusted Networks", RFC 3325, November 2002.

[RFC3327] Willis, D. and B. Hoeneisen, "Session Initiation Protocol (SIP) Extension Header Field for Registering Non-Adjacent Contacts", RFC 3327, December 2002.

[RFC3455] Garcia-Martin, M., Henrikson, E., and D. Mills, "Private Header (P-Header) Extensions to the Session Initiation Protocol (SIP) for the 3rd-Generation Partnership Project (3GPP)", RFC 3455, January 2003.

[RFC3966] Schulzrinne, H., "The tel URI for Telephone Numbers", RFC 3966, December 2004.

[RFC4244] Barnes, M., "An Extension to the Session Initiation Protocol (SIP) for Request History Information", RFC 4244, November 2005.

[RFC5626] Jennings, C., Mahy, R., and F. Audet, "Managing Client-Initiated Connections in the Session Initiation Protocol (SIP)", RFC 5626, October 2009.

[RFC5627] Rosenberg, J., "Obtaining and Using Globally Routable User Agent URIs (GRUUs) in the Session Initiation Protocol (SIP)", RFC 5627, October 2009.

[3GPP.23.003] 3GPP, "Numbering, addressing and identification", 3GPP TS 23.003 3.15.0, October 2006.

[3GPP.24.229] 3GPP, "IP multimedia call control protocol based on Session Initiation Protocol (SIP) and Session Description Protocol (SDP); Stage 3", 3GPP TS 24.229 10.0.0, June 2010.

[ETSI_TS_182025] ETSI TS 182 025, "Telecommunications and Internet converged Services and Protocols for Advanced Networking (TISPAN); Business trunking; Architecture and functional description".

Authors' Addresses

John Elwell
Siemens Enterprise Communications

EMail: john.elwell@siemens-enterprise.com

Hadriel Kaplan
Acme Packet
71 Third Ave.
Burlington, MA 01803
USA

EMail: hkaplan@acmepacket.com