

SIP
Internet-Draft
Intended status: Informational
Expires: August 28, 2008

D. Schwartz
XConnect
H. Kaplan
Acme Packet
K. Darilion
enum.at
H. Tschofenig
Nokia Siemens Networks
February 25, 2008

E.164 Ownership Problem Statement
draft-schwartz-sip-e164-ownership-01.txt

Status of this Memo

By submitting this Internet-Draft, each author represents that any applicable patent or other IPR claims of which he or she is aware have been or will be disclosed, and any of which he or she becomes aware will be disclosed, in accordance with [Section 6 of BCP 79](#).

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF), its areas, and its working groups. Note that other groups may also distribute working documents as Internet-Drafts.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

The list of current Internet-Drafts can be accessed at <http://www.ietf.org/ietf/lid-abstracts.txt>.

The list of Internet-Draft Shadow Directories can be accessed at <http://www.ietf.org/shadow.html>.

This Internet-Draft will expire on August 28, 2008.

Copyright Notice

Copyright (C) The IETF Trust (2008).

Abstract

When a call travels end-to-end relayed from the PSTN to SIP then problems occur with E.164 number ownership. Additionally, there are security challenges when the PSTN-VoIP gateway has to authenticate

and authorize the calling party. Without addressing these two aspects the overall security story is weak or non-existent. This document aims to investigate these two aspect; it does, however, not investigate current E.164 number handling with [RFC 4474](#) ("SIP Identity"). Such an analysis is provided by other documents already.

Table of Contents

1.	Introduction	3
2.	Terminology	3
3.	The End-to-End Picture	3
3.1.	IP-IP Case	4
3.2.	IP-PSTN-IP Case	5
3.3.	PSTN-to-IP Case	5
3.4.	IP-to-PSTN Case	6
4.	Authenticating and Authorizing the Calling Party Identity . .	7
5.	Verifying Ownership: What does it mean?	8
6.	Security Considerations	11
7.	Contributors	11
8.	IANA Considerations	12
9.	Acknowledgments	12
10.	References	12
10.1.	Normative References	12
10.2.	Informative References	12
	Authors' Addresses	13
	Intellectual Property and Copyright Statements	15

1. Introduction

[RFC 4474](#) [2] defines a mechanism whereby an authentication service asserts the identity of a SIP UAC and determines whether he or she is authorized to use that identity. The authentication service then computes a hash over some particular headers, including the From header field and the bodies in the message. This hash is signed with the certificate for the domain and inserted in the 'Identity' header field in the SIP message. The proxy also inserts a companion header field, Identity-Info, that tells the verifying party how to acquire its certificate, in case it is not yet known already.

When the verifier receives the SIP message, it verifies the signature provided in the Identity header, and thus can determine whether the domain indicated by the host portion of the AoR in the From header field authenticated the user, and permitted the user to assert that From header field value.

The use of phone numbers with SIP was introduced with the TEL URL scheme [4] whereby domain names were not used with the phone numbers. SIP URIs always have domain names. In SIP [1], a translation between SIP URIs and TEL URLs is described: when translating from a SIP URI to a TEL URL, the domain name from the SIP URI is simply dropped. When translating in the other direction (or simply generating a SIP URI from an E.164 number [13]) it is not clear how to populate the domain name.

When SIP Identity [2] is applied to E.164 numbers then there is the question what the identity assertion actually means. Additionally, the usage of the domain for an E.164 number causes problems, as described in [6]. This document will, however, not focus on this aspect. Instead, we investigate the overall end-to-end security story and the ownership problem for E.164 numbers.

2. Terminology

This document largely relies on the terminology introduced by [2].

3. The End-to-End Picture

In the context of "ownership" it is hard to speak of the end-to-end picture without first identifying four possible use-cases for this e2e communication. The first two start AND end on IP and the second two start OR end on IP. Please refer to Figure 1 below for the first two cases.

Schwartz, et al.

Expires August 28, 2008

[Page 3]

Internet-Draft

E.164 Ownership Problem Statement

February 2008

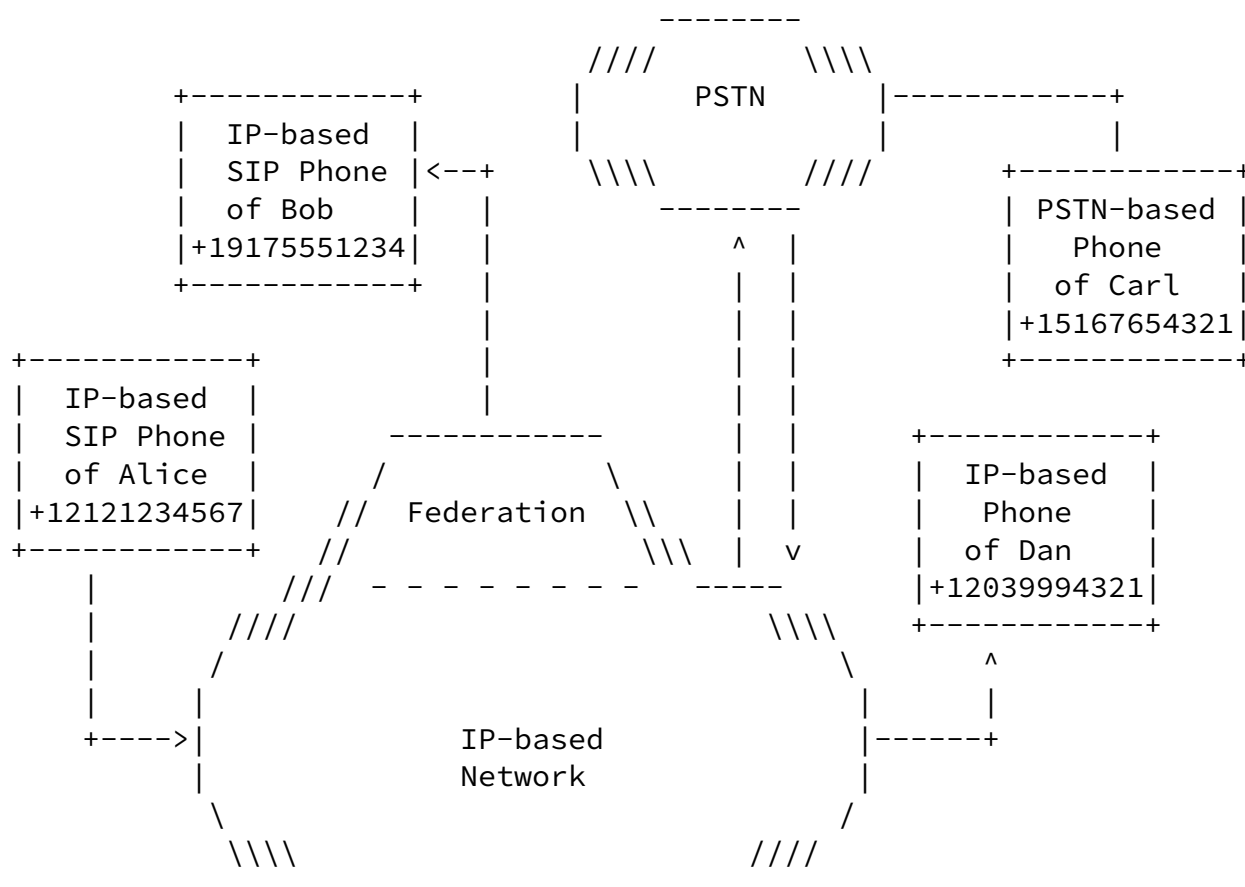


Figure 1: Federation based IP-to-IP Communication

3.1. IP-IP Case

The first use case is that of a call that originates and terminates on the IP network without ever touching the PSTN but that uses E.164 addressing instead of the preferred URI. This case is quite prevalent today in some of the private peering federations. These federations are seen as a first choice (if I can terminate to an IP great - otherwise let me know and I will failover or route advance to the PSTN) for outbound routing of E.164 numbers. Since these federations are being used in conjunction with the PSTN it is quite logical that the addressing will be E.164 and not SIP URI based.

As can be seen in Figure 1 if Alice calls Bob the call will be IP based end-to-end while if she calls Carl it will exit to the PSTN. Ownership, therefore needs to be considered in the context of this use-case. Does the COR play any role in this case? Can these numbers be treated as private plan numbers placing all onus solely on the respective VSPs servicing Alice and Bob?

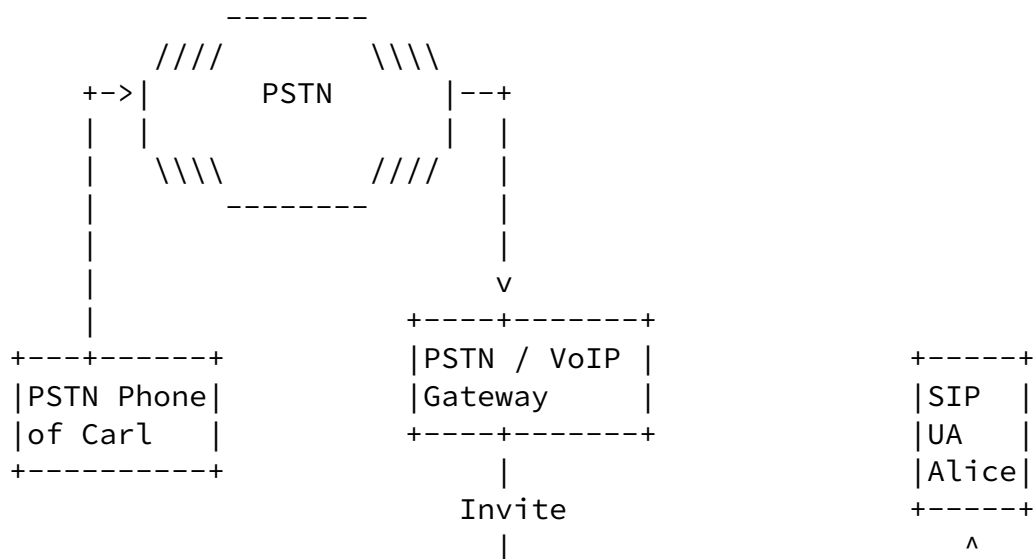
[3.2.](#) IP-PSTN-IP Case

In this case Dan's VSP is not a member of the federation that is shared by Alice and Bob and as such so far as Alice is concerned Dan is not accessible via IP.

What considerations should be discussed in this case? In reality both origination and termination are IP, however, the transit is PSTN and who know what happens in that world. What is the notion of ownership here? Since any "domain" information will be stripped by the PSTN is there any advantage whatsoever to including it?

[3.3.](#) PSTN-to-IP Case

Consider Figure 2 where Carl is using a PSTN phone and initiates calls to Alice. Alice is using an IP-based phone. The call of Carl traverses the PSTN and enters the Internet via some PSTN/VoIP gateway. This gateway applies SIP Identity to the call. What does the signed identity mean? Can the gateway in typical deployment cases verify the caller id in any meaningful way? Later, when Alice's SIP UA receives the call it may run some authorization procedure against the received identity. It may "outsource" the



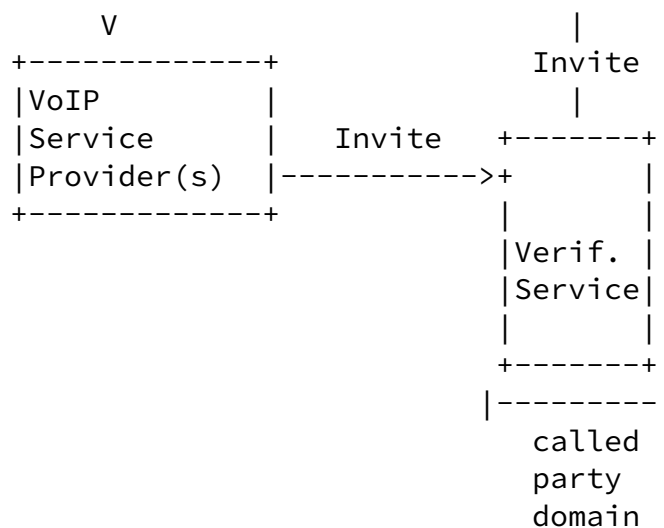
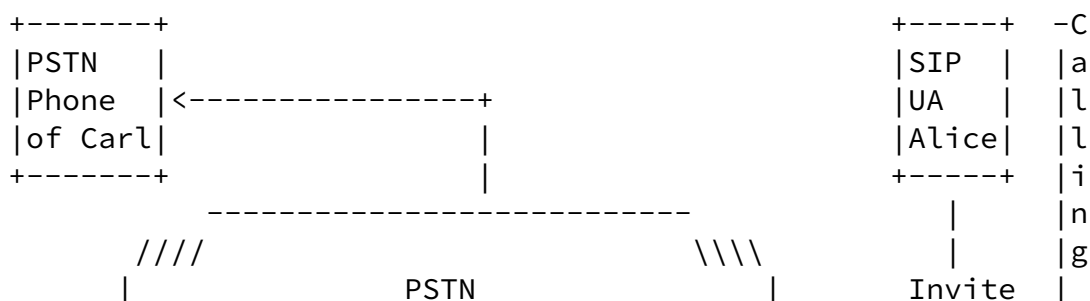


Figure 2: PSTN-to-IP Communication

3.4. IP-to-PSTN Case

Consider Figure 3 where Alice calls Carl. Carl uses a PSTN phone and Alice an IP-based phone. When Alice initiates the call the E.164 number needs to get translated, for example using ENUM, to a SIP URI and subsequently to an IP address. The call of Alice traverses her VoIP provider where the SIP Identity signature is added. It then hits the PSTN/VoIP gateway. What would the gateway do with the SIP Identity header? Can he do anything meaningful with it? Ideally, Alice would like to know whether she, for example, talks to someone at her bank rather than to someone intercepting the call. Would Connected Identity help her? What would the quality of the subsequently established media security between the gateway and Alice's SIP UA be?



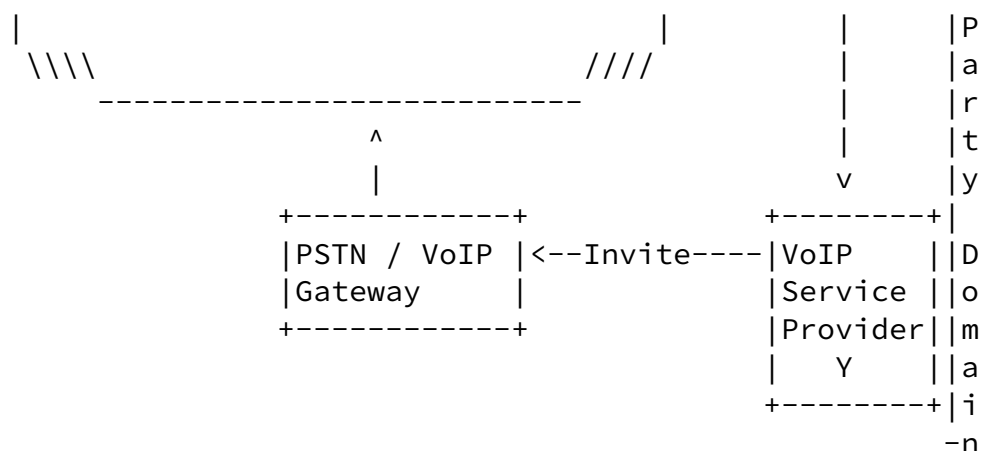


Figure 3: IP-to-PSTN Communication

4. Authenticating and Authorizing the Calling Party Identity

[RFC 4474](#) rightfully makes some important assumptions about the behavior of the authentication service that contribute significantly to the security of the overall system. While some assumptions seem to be obvious for SIP usage, they are less obvious when considering them in relationship with a PSTN interworking or E.164 number usage. Section 4 of [\[2\]](#) says:

"The authentication service authenticates Alice (possibly by sending a Digest authentication challenge) and validates that she is authorized to assert the identity that is populated in the From header field. This value may be Alice's AoR, or it may be some other value that the policy of the proxy server permits her to use.

...

The proxy, as the holder of the private key of its domain, is asserting that the originator of this request has been authenticated and that she is authorized to claim the identity (the SIP address- of-record) that appears in the From header field. "

The crucial question therefore is: In the generic case is the

authentication service able to authenticate the caller-ID used in the PSTN and to authorize it's usage?

There are problems with this step:

1. The PSTN builds on a walled garden with a chain-of-trust security model. This is "nice" as long as the participating parties are indeed honest. Unfortunately, this is not true anymore (and has not been the case for a long time already) [add-references]. Caller-ID spoofing is common and even transit providers are not trustworthy either.
2. A call originated on the PSTN is often times routed to a PSTN/VoIP gateway. That PSTN gateway is operated by the owner of the called number, rather than the owner of the calling number.

5. Verifying Ownership: What does it mean?

Imagine a verification service at Alice's VoIP provider network receives a SIP message with an 'Identity' and an 'Identity-Info' header.

When the username and the domain name are tightly bound together then there is no question whether a particular authentication service operating at a specific domain is administratively responsible for a specific username part. However, if this binding is relaxed or even removed then there is a question of which authentication service is allowed to warrant for which usernames.

Ownership is an artificial construct but one could compare it with an oracle that returns the name of a domain when asked who is authoritative for using a particular E.164 number.

The problem is compounded by the fact that there may be more than one legitimate owner. Consider if you will the case where an enterprise (PBX) uses a Voice Service Provider (VSP) for IP communication services and the VSP acquires E.164 numbers from an exchange who in turn acquires the numbers from the Carrier of Record (COR). This is illustrated in Figure 4.

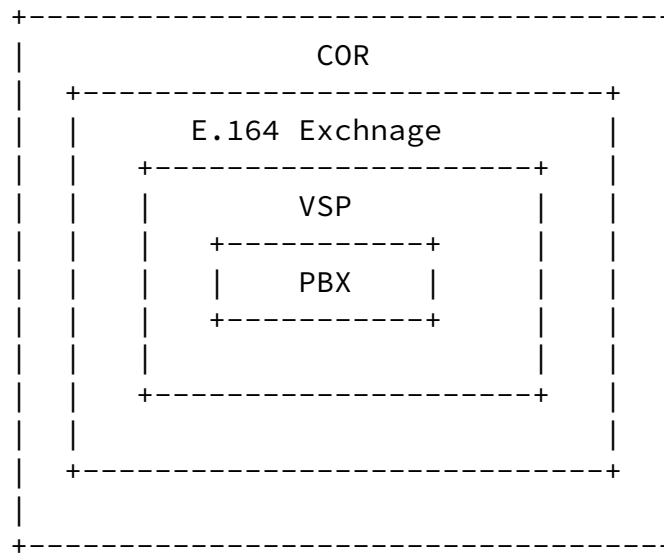


Figure 4: Will the real 'Owner' please stand up?

If one was to compare this to the path validation approach used in chain-of-trust certificate validation schemes, the COR would be the trust anchor and would sign the exchange cert who in turn would sign the VSP cert who in turn would sign the PBX cert which would be used in 4474 [2]. While the steps needed to traverse up the chain and check all the certs are seemingly quite expensive (performance wise for calls at least) one must realize that calling patterns are quite deterministic and as such caching is believed to alleviate this issue and make it tolerable. Without this chain-of-trust approach it is hard to give credibility to any "ownership" assertion.

Looking at "ownership" in this way may necessitate an Authority Information Access (AIA) [11] equivalent so that a URI scoping an E.164 number would provide the pointer back up the tree for complete validation. If the number is ported from one COR to another all that would be needed is to modify the AIA information starting with the anchor and down to where relevant.

There are various ownership verification steps that got used in the IETF within other protocols. RFC 4474 [2], for example, uses the following verification step for SIP URIs:

"6. Verifier Behavior

Step 2:

The verifier MUST follow the process described in [Section 13.4](#) to

determine if the signer is authoritative for the URI in the From header field.

13.4. Domain Names and Subordination

When a verifier processes a request containing an Identity-Info header, it must compare the domain portion of the URI in the From header field of the request with the domain name that is the subject of the certificate acquired from the Identity-Info header."

This is a concept of referential integrity where information of the protocol (in this case the identity) is matched against information from the certificate. The signer and the verifier need to have a trust anchor in common. There are additional aspects about the detailed matching procedure that are described in Section 13.4 of [\[2\]](#).

Unfortunately, this simple authorization check cannot be used with E.164 numbers because of the missing domain concept in the identifier itself and because of number portability. Imagine if the SIP Identity authentication service would have to sign calling parties SIP URIs that do not belong to the domain the authentication service is responsible for. The corresponding verification check would be far more complicated -- the authentication service would have to show that it is indeed entitled to act on behalf of someone else.

A couple of other ownership approaches have been used in IETF protocols. These examples are not meant to claim that the problem is easy to solve (in the style of just pick one) or that there is even a satisfactory solution at all. They are just listed to illustrate the different flavors and the quality of the warrants:

Return Routability Check: A form of check is to exploit the topological properties of identifier routing and the possible placements of adversaries with respect to a certain message interaction. RRT and various other forms fall into that category. An example can be found in [\[8\]](#).

Authorization Certificates:

A form of check is to use authorization certificates. The basic idea is that one would trust the entity that creates the authorization certificate (most likely in a hierarchical form) then you also trust its content. SIP-SAML (see [7]) and [12] belong to this category. When the identity of the certificate is constructed in a suitable way then together with a delegated signing the same effect could be accomplished.

Distributed Databases:

Another form of mechanism is to use an out-of-band database lookup, for example using the DNS, in order to verify that the entity which uses the private key for creating the SIP Identity header is authorized to attach the corresponding public key to the this distributed database. The identity would be used for the lookup to the database and the security of the system relies on ensuring that only those entities add the public key that are also owner of the corresponding E.164 number. An example of such an approach can be found in [15]. The usage of TRIP [10] (with extensions with information about E.164 numbers that are authorized for usage by a specific provider) has been discussed as well.

Cryptographic Addresses and Hash Chains:

These mechanisms utilize a temporal property by creating a binding between the public key (or values from a hash chain) and the identity be verified by re-computing the hash value and by comparing the hash with the identifier. These mechanisms have found some excitement with protocol work at lower layers (see, for example, [9]).

Needless to say that each mechanism has different scalability, security and deployment properties.

[6.](#) Security Considerations

With the work on this subject it is important to keep two quotes in mind:

- o "The security of a system is as good as the weakest link."
- o "If you think cryptography is the solution to your problem, you don't know what your problem is." --- Roger Needham

The authors argue that the problem scope and the envisioned technical properties are not yet understood enough. Furthermore, it is necessary to investigate deployment challenges imposed by the existing infrastructure and deployment incentives for various approaches.

7. Contributors

We would like to thank the following individuals for their contributions to this document:

Schwartz, et al. Expires August 28, 2008 [Page 11]

Internet-Draft E.164 Ownership Problem Statement February 2008

- o Dan Wing
- o John Elwell
- o Kai Fischer

8. IANA Considerations

There are no IANA considerations with this document.

9. Acknowledgments

We would like to thank Joel M. Halpern, Paul Kyzivat, Dale Worley, Jonathan Rosenberg, and Henry Sinnreich for their feedback on the mailing list.

10. References

10.1. Normative References

- [1] 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.

- [2] Peterson, J. and C. Jennings, "Enhancements for Authenticated Identity Management in the Session Initiation Protocol (SIP)", [RFC 4474](#), August 2006.
- [3] Allman, E., Callas, J., Delany, M., Libbey, M., Fenton, J., and M. Thomas, "DomainKeys Identified Mail (DKIM) Signatures", [RFC 4871](#), May 2007.
- [4] Schulzrinne, H., "The tel URI for Telephone Numbers", [RFC 3966](#), December 2004.
- [5] Faltstrom, P. and M. Mealling, "The E.164 to Uniform Resource Identifiers (URI) Dynamic Delegation Discovery System (DDDS) Application (ENUM)", [RFC 3761](#), April 2004.

[10.2.](#) Informative References

- [6] Elwell, J., "SIP E.164 Problem Statement", [draft-elwell-sip-e164-problem-statement-00](#) (work in progress), February 2008.
- [7] Tschofenig, H., Hodges, J., Peterson, J., Polk, J., and D. Sicker, "SIP SAML Profile and Binding", [draft-ietf-sip-saml-03](#)

(work in progress), November 2007.

- [8] Wing, D., "SIP E.164 Return Routability Check (RRC)", [draft-wing-sip-e164-rrc-01](#) (work in progress), February 2008.
- [9] Aura, T., "Cryptographically Generated Addresses (CGA)", [RFC 3972](#), March 2005.
- [10] Rosenberg, J., Salama, H., and M. Squire, "Telephony Routing over IP (TRIP)", [RFC 3219](#), January 2002.
- [11] Housley, R., Ford, W., Polk, T., and D. Solo, "Internet X.509 Public Key Infrastructure Certificate and CRL Profile", [RFC 2459](#), January 1999.
- [12] Bellovin, S., Ioannidis, J., Keromytis, A., and R. Stewart, "On the Use of Stream Control Transmission Protocol (SCTP) with IPsec", [RFC 3554](#), July 2003.

- [13] ITU-T, "The international public telecommunication numbering plan", Recommendation E.164, May 1997.
- [14] Peterson, J., "A Privacy Mechanism for the Session Initiation Protocol (SIP)", [RFC 3323](#), November 2002.
- [15] Darilion, K. and H. Tschofenig, "E.164 Ownership using Public Keys stored in ENUM", [draft-darilion-sip-e164-enum-00](#) (work in progress), February 2008.

Authors' Addresses

David Schwartz
XConnect
Malcha Technology Park
Jerusalem, 96951
Israel

Email: dschwartz@xconnect.net

Schwartz, et al.

Expires August 28, 2008

[Page 13]

Internet-Draft

E.164 Ownership Problem Statement

February 2008

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

Phone:
Fax:
Email: hkaplan@acmepacket.com
URI:

Klaus Darilion
enum.at GmbH
Karlsplatz 1/9
Wien A-1010
Austria

Phone: +43 1 5056416 36
Email: klaus.darilion@enum.at
URI: <http://www.enum.at/>

Hannes Tschofenig
Nokia Siemens Networks
Linnoitustie 6
Espoo 02600
Finland

Phone: +358 (50) 4871445
Email: Hannes.Tschofenig@nsn.com
URI: <http://www.tschofenig.com>

This document is subject to the rights, licenses and restrictions contained in [BCP 78](#), and except as set forth therein, the authors retain all their rights.

This document and the information contained herein are provided on an "AS IS" basis and THE CONTRIBUTOR, THE ORGANIZATION HE/SHE REPRESENTS OR IS SPONSORED BY (IF ANY), THE INTERNET SOCIETY, THE IETF TRUST AND THE INTERNET ENGINEERING TASK FORCE DISCLAIM ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO ANY WARRANTY THAT THE USE OF THE INFORMATION HEREIN WILL NOT INFRINGE ANY RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Intellectual Property

The IETF takes no position regarding the validity or scope of any Intellectual Property Rights or other rights that might be claimed to pertain to the implementation or use of the technology described in this document or the extent to which any license under such rights might or might not be available; nor does it represent that it has made any independent effort to identify any such rights. Information on the procedures with respect to rights in RFC documents can be found in [BCP 78](#) and [BCP 79](#).

Copies of IPR disclosures made to the IETF Secretariat and any assurances of licenses to be made available, or the result of an attempt made to obtain a general license or permission for the use of such proprietary rights by implementers or users of this specification can be obtained from the IETF on-line IPR repository at <http://www.ietf.org/ipr>.

The IETF invites any interested party to bring to its attention any copyrights, patents or patent applications, or other proprietary rights that may cover technology that may be required to implement this standard. Please address the information to the IETF at ietf-ipr@ietf.org.

Acknowledgment

Funding for the RFC Editor function is provided by the IETF Administrative Support Activity (IASA).