

ecrit
Internet-Draft
Expires: November 2, 2005

H. Schulzrinne
Columbia U.
R. Marshall, Ed.
TCS
May 2005

Requirements for Emergency Context Resolution with Internet Technologies [draft-schulzrinne-ecrit-requirements-01](#)

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 November 2, 2005.

Copyright Notice

Copyright (C) The Internet Society (2005).

Abstract

This document enumerates requirements for emergency calls placed by the public using voice-over-IP (VoIP) and general Internet multimedia systems, where Internet protocols are used end-to-end.

Internet-Draft

ECRIT requirements

May 2005

Table of Contents

1.	Introduction	3
2.	Terminology	5
3.	High-Level Requirements	9
4.	Emergency Address	11
5.	Identifying the Caller Location	12
6.	Identifying the Appropriate PSAP	13
7.	Emergency Address Directory	16
8.	Supplemental Information	17
9.	Security Considerations	18
10.	Contributors	19
11.	Acknowledgments	20
12.	References	21
12.1	Normative References	21
12.2	Informative References	21
	Authors' Addresses	21
	Intellectual Property and Copyright Statements	23

1. Introduction

Users of telephone-like services expect to be able to call for emergency help, such as police, the fire department or an ambulance, regardless of where they are, what (if any) service provider they are using and what kind of device they are using. Unfortunately, the mechanisms for emergency calls that have evolved in the public circuit-switched telephone network (PSTN) are not quite appropriate for evolving IP-based voice, text and real-time multimedia communications. This document outlines the key requirements that end systems and network elements such as SIP proxies need to satisfy in order to provide emergency call services that offer at least the same functionality as existing PSTN services, with the goal of making emergency calling more robust, cheaper to implement and multimedia-capable.

In the future, users of other real-time and near real-time services may also expect to be able to summon emergency help. For example, instant messaging (IM) users may want to use such services. IM is particularly helpful for hearing-disabled users ([RFC 3351](#) [4]) and in cases where bandwidth is scarce.

This document only focuses on end-to-end IP-based calls, i.e., where the emergency call originates from an IP end system, (Internet device), and terminates to an IP-capable PSAP, done entirely over an IP network.

This document identifies functional and security issues for determining the correct emergency identifier, for identifying the appropriate PSAP (emergency address) and for identifying the caller and its current location.

Emergency calls need to be identified ([Section 6](#)). Emergency identifiers are used by the emergency caller to declare a call to be an emergency call. The device MUST recognize the emergency identifiers used and convert them to an emergency address to guide

the call to a PSAP. The emergency address MUST be a predefined "sip", "sips" or "tel" URI scheme.

Emergency calls need to be routed to the appropriate PSAP (ref. [Section 6](#)). Several terms are used for causing the call signaling to reach the geographically appropriate PSAP. This has been referred to as call routing, (PSAP) lookup or location mapping, all capturing aspects of the problem.

Emergency calls need to identify who placed the call ([Section 7](#)). In most jurisdictions, callers do not have a choice as to whether they want to reveal their location or identity; such disclosure is

typically mandated by law.

Emergency calls need to identify the location from which the call is initiated ([Section 5](#)). The caller location needs to be identified for two purposes, namely to route the call to the appropriate PSAP and to display the caller location to the call taker to simplify dispatching emergency assistance to the correct location.

Emergency calls may not be subject to access restrictions placed on non-emergency calls. Also, some call features may interfere with emergency calls, particularly if triggered accidentally ([Section 7](#)).

[2.](#) Terminology

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](#) [1] and indicate requirement levels for compliant implementations.

Since a requirements document does not directly specify an implementable protocol, these compliance labels should be read as indicating requirements for the protocol or architecture, rather than an implementation.

For lack of a better term, we will use the term "caller" or "emergency caller" to refer to the person placing an emergency call or sending an emergency IM.

Access Infrastructure Provider (AIP): An organization that provides physical network connectivity to its customers or users, e.g. through digital subscriber lines, cable TV plants, Ethernet, leased lines or radio frequencies. This entity may or may not also provide IP routing, IP addresses, or other Internet protocol services. Examples of such organizations include

telecommunication carriers, municipal utilities, larger enterprises with their own network infrastructure, and government organizations such as the military.

[Ed. AIP vs. IAP vs. ? not yet clear as to general agreement on a single term.]

address: A description of a location of a person, organization, or building, most often consisting of numerical and text elements such as street number, street name, and city arranged in a particular format.

administrative domain: An area or group of services falling within a specific category or jurisdictional boundary.

Application (Voice) Service Provider (ASP, VSP): The organization that provides voice or other application-layer services, such as call routing, a SIP URI or PSTN termination. This organization can be a private individual, an enterprise, a government or a service provider. We avoid the term voice service provider as emergency calls are likely to use other media, including text and video, in the future. For a particular user, the ASP may not be the same organization as the AIP or ISP.

Basic Emergency Service: Basic Emergency Service allows a user to reach a PSAP serving its current location, but the PSAP may not be able to determine the identity or geographic location of the caller (except by having the call taker ask the caller).

call taker: A call taker is an agent at the PSAP that accepts calls and may dispatch emergency help. (Sometimes the functions of call taking and dispatching are handled by different groups of people, but these divisions of labor are not generally visible to the outside and thus do not concern us here.)

civic location: A described location based on some defined grid, such as a jurisdictional, postal, metropolitan, or rural reference system (e.g. street address).

domain authentication and validation entity: A node that has authority within a given domain to authenticate and validate user location information.

Emergency Control Center (ECC): Facilities used by emergency organizations to accept and handle emergency calls. A PSAP (below) forwards emergency calls to the emergency control center, which dispatches police, fire, rescue and other emergency services. An ECC serves a limited geographic area. A PSAP and ECC can be combined into one facility (ETSI SR 002 180 definition). We assume that the ECC is reachable by IP-based protocols, such as SIP for call signaling and RTP for media.

emergency address: The sip:uri, sips:uri, or tel:uri which represents the network address of the PSAP useful for the completion of a VoIP emergency call.

emergency caller: The user or user device entity which sends his/her location to another entity in the network.

emergency identifier: The numerical and/or text identifier which is supplied by a user or a user device, which identifies the call as an emergency call and is translated into an emergency address for call routing and completion.

enhanced emergency service: Enhanced emergency services add the ability to identify the caller identity and/or caller location to basic emergency services. (Sometimes, only the caller location may be known, e.g. from a public access point that is not owned by an individual.)

ESRP (Emergency Services Routing Proxy): An ESRP is a call routing entity that invokes the location-to-URL mapping, which in turn may return either the URL for another ESRP or the PSAP. (In a SIP system, the ESRP would typically be a SIP proxy, but could also be a Back-to-back user agent (B2BUA).

geocoding: The process of finding the location of a street address on a map. The location can be an x,y coordinate or a feature such as

a street segment, postal delivery location, or building. In GIS, geocoding requires a reference dataset that contains address attributes for the geographic features in the area of interest.

geographic coordinates: A representation (measurement) of a location on the earth's surface expressed in degrees of latitude and longitude.

geographic coordinate system: A reference system that uses latitude and longitude to define the locations of points on the surface of a sphere or spheroid.

geographic transformation: A method of converting data between two geographic coordinate systems (datums).

geographic location: A reference to a locatable point described by a set of defined coordinates within a geographic coordinate system, (e.g. lat/lon within WGS-84 datum)

Internet Service Provider (ISP): An organization that provides IP network-layer services to its customers or users. This entity may or may not provide the physical-layer and layer-2 connectivity, such as fiber or Ethernet.

location: A geographic identification assigned to a region or feature based on a specific coordinate system, or by other precise information such as a street address. In the geocoding process, the location is defined with an x,y coordinate value according to the distance north or south of the equator and east or west of the prime meridian.

Location Key (LK): A key identifier used to query a location server in order to retrieve a specific end user or end user device location.

location validation: A caller location is considered valid if the civic or geographic location is recognizable within an acceptable location reference systems (e.g. USPS, WGS84, etc.), and can be mapped to one or more PSAPs. Location validation ensures that a location is reference able, but makes no assumption about the

association between the caller and the caller's location.

PSAP (Public Safety Answering Point): Physical location where emergency calls are received under the responsibility of a public authority. (This terminology is used by both ETSI, in ETSI SR 002 180, and NENA.) In the United Kingdom, PSAPs are called Operator Assistance Centres, in New Zealand Communications Centres. Within this document, it is assumed, unless stated otherwise, that PSAP is that which supports the receipt of emergency calls over IP. It is also assumed that the PSAP is reachable by IP-based protocols, such as SIP for call signaling and RTP for media.

x,y coordinates: A pair of values that represents the distance from an origin (0,0) along two axes, a horizontal axis (x) representing east-west, and a vertical axis (y) representing north-south. On a map, x,y coordinates are used to represent features at the location they are found on the earth's spherical surface.

3. High-Level Requirements

Below, we summarize high-level architectural requirements that guide some of the component requirements detailed later in the document.

- R1. Application Service Provider: The existence of a Application Service Provider (ASP) MUST NOT be assumed.

Motivation: The caller may not have a voice service provider, i.e., a corporate entity that provides voice services as a business. For example, a residence may have its own DNS domain and run its own SIP proxy server for that domain. On a larger scale, a university might provide voice services to its students and staff, but not be a telecommunication provider.

- R2. International: The protocols and protocol extensions developed MUST support regional, political and organizational differences.

Motivation: It MUST be possible for a device or software developed or purchased in one country to place emergency calls in another country. System components should not be biased towards a particular set of emergency numbers or languages. Also, different countries have evolved different ways of organizing emergency services, e.g. either centralizing them or having smaller regional subdivisions such as United States counties or municipalities handle emergency calls.

- R3. Distributed Administration: Deployment of emergency services MUST NOT depend on a sole central administration authority.

Motivation: Once common standards are established, it must be possible to deploy and administer emergency calling features on a regional or national basis without requiring coordination with other regions or nations. The system cannot assume, for example, that there is a single global entity issuing certificates for PSAPs, ASPs, AIPs or other participants.

- R4. Multiple Modes: Multiple communication modes, including Multimedia data and services MUST be supported.

Motivation: Emergency calling must support a variety of media, not just voice and TDD (telecommunication device for the deaf) beyond the capabilities of current limitations. Such additional media should include conversational text, instant messaging and video. In addition, it should be possible to convey telemetry data, such as data from automobile crash sensors.

- R5. Minimum Connectivity: An emergency call should succeed as long as there is a working network path between the caller and the PSAP. In particular, reliance during call set-up and calls on entities and network paths that are located elsewhere should be minimized.

Example: A caller in New York who needs to contact a PSAP in the same city shouldn't have to get information from some entity in Texas to make that call, as the call would then fail if the New York to Texas path is unavailable. (To avoid this, the caller could, for example, have cached mapping information, use a local server that has the necessary information, or use other mechanisms to avoid such off-path dependencies.)

[Ed. No resolution yet agreed to for the above requirement.]

- R6. Incremental Deployment The output of the ECRIT mapping protocol will be one or more URIs that can be used as the target of an emergency communication. These must be usable by an appropriately capable device even if that device has no knowledge of the mapping protocol. As an example, if the mapping protocol returns a SIP URI any SIP-capable phone should be able to use it as a target of the call; no special extension to SIP should be required.

[4.](#) Emergency Address

- A1. Universal: Each device and all network elements MUST recognize one or more universal (global) emergency identifiers, regardless of the location of the device, the service provider used (if any) or other factors. Examples of these might include: 911, 112, and sos.*

Motivation: SIP and other call signaling protocols are not specific to one country or service provider and devices are likely to be used across national or service provider boundaries. Since services such as disabling mandatory authentication for emergency calls requires the cooperation of outbound proxies, the outbound proxy has to be able to recognize the emergency address and be assured that it will be routed as an emergency call. Thus, a simple declaration on a random URI that it is an emergency call will likely lead to fraud and possibly attacks on the network infrastructure. A universal address also makes it possible to create user interface elements that are correctly configured without user intervention. UA features could be made to work without such an identifier, but the user interface would then have to provide an unambiguous way to declare a particular call an emergency call.

- A3. Recognizable: Emergency calls MUST be recognizable by user agents, proxies and other network elements. To prevent fraud, an address identified as an emergency number for call features or authentication override MUST also cause routing to a PSAP.
- A4. Minimal configuration: Any local emergency identifiers SHOULD be configured automatically, without user intervention.

Motivation: A new UA "unofficially imported" into an organization from elsewhere should have the same emergency capabilities as one officially installed.

- A6. Backwards-compatible: Existing devices that predate the specification of emergency call-related protocols and conventions MUST be able reach a PSAP.

[5.](#) Identifying the Caller Location

This section supplements the requirements outlined in [RFC 3693](#) [5]. Thus, the requirements enumerated there are not repeated here. In general, we can distinguish three modes of operation:

UA-inserted: The caller's user agent inserts the location information, derived from sources such as GPS, DHCP or link-layer announcements (LLDP).

UA-referenced: The caller's user agent provides a reference, via a permanent or temporary identifier, to the location which is stored by a location service somewhere else and then retrieved by the PSAP.

Proxy-inserted: A proxy along the call path inserts the location or location reference.

- L6. Validation of civic location: It MUST be possible to validate an address prior to its use in an actual emergency call.

Motivation: Location validation refers to a process to determine whether or not a given civic location is valid or not. A location is said to be valid if it can be mapped exactly to a unique emergency address for a PSAP, known to the emergency services

directory/mapping database.

L10. Preferred datum: The preferred geographic coordinate system for emergency calls SHALL be WGS-84.

L28. Location Provided: If location is provided to the routing proxy, it MUST be provided to the PSAP.

Motivation: Transmission of the current location of the contacting device to the PSAP.

[6.](#) Identifying the Appropriate PSAP

From the previous section, we take the requirement of a single (or small number of) emergency addresses which are independent of the caller's location. However, since for reasons of robustness, jurisdiction and local knowledge, PSAPs only serve a limited geographic region, having the call reach the correct PSAP is crucial. While a PSAP may be able to transfer an errant call, any such transfer is likely to add tens of seconds to call setup latency and is prone to errors. (In the United States, there are about 6,100 PSAPs.)

There appears to be two basic architectures for translating an emergency identifier into the correct PSAP emergency address. We refer to these as caller-based and mediated. In caller-based resolution, the caller's user agent consults a directory and determines the correct PSAP based on its location. We assume that the user agent can determine its own location, either by knowing it

locally or asking some third party for it. A UA could conceivably store a complete list of all PSAPs across the world, but that would require frequent synchronization with a master database as PSAPs merge or jurisdictional boundaries change.

For mediated resolution, a call signaling server, such as a SIP (outbound) proxy or redirect server performs this function. Note that the latter case includes the architecture where the call is effectively routed to a copy of the database, rather than having some non-SIP protocol query the database. Since servers may be used as outbound proxy servers by clients that are not in the same geographic area as the proxy server, any proxy server has to be able to translate any caller location to the appropriate PSAP. (A traveler may, for example, accidentally or intentionally configure its home proxy server as its outbound proxy server, even while far away from home.)

The resolution may take place well before the actual emergency call is placed, or at the time of the call.

The problem is harder than for traditional web or email services. There, the originator knows which entity it wants to reach, identified by the email address or HTTP URL. However, the emergency caller only dialed an emergency identifier. Depending on the location, any of several ten thousand PSAPs around the world could be valid. In addition, the caller probably does not care which specific PSAP answers the call, but rather that it be an accredited PSAP, e.g. one run by the local government authorities. (Many PSAPs are run by private entities. For example, universities and corporations with large campuses often have their own emergency response centers.)

- I1. Correct PSAP: Calls Must be routed to the PSAP responsible for this particular geographic area.

Motivation: In particular, the location determination should not be fooled by the location of IP telephony gateways or dial-in lines into a corporate LAN (and dispatch emergency help to the gateway or campus, rather than the caller), multi-site LANs and similar arrangements.

- I3. Multi-stage resolution: A mapping server for a large geographic area SHOULD be able to refer clients to mapping servers

responsible for subsets of the geographic area.

Motivation: In some cases, an initial mapping may provide a single URL for a large geographic area. The ESRP identified by that URL then re-invokes the mapping protocol on a different database to obtain another URL for an ESRP or PSAP covering a smaller area.

- I4. Return multiple PSAPs: The mapping protocol MUST be able to return multiple URLs for different PSAPs that cover the same area.

The mapping protocol MUST provide additional information that allows the querying entity to determine relevant properties of the URL.

Motivation: In some cases, the same geographic area is served by several PSAPs, for example, a corporate campus might be served by both a corporate security department and the municipal PSAP. The mapping protocol should then return URLs for both, with information allowing the querying entity to choose one or the other. The choice would typically be made by an ESRP based on local policy, not by a human user.

- I7. Traceable resolution: The entity requesting mapping SHOULD be able to definitively and securely determine the entity or entities who provided the emergency address resolution information.
- I8. Resilience against server failure: A client MUST be able to fail over to another replica of the mapping server, so that a failure of a server does not endanger the ability to perform the mapping.
- I10. Incrementally deployable: The mapping function MUST be capable of being deployed incrementally. It must not be necessary, for example, to have a global street level database before deploying the system. It is acceptable to have some misrouting of calls when the database does not (yet) contain accurate boundary information.

- I13. Existing infrastructure support: It SHOULD be possible for the mapping function to provide information that allows the requesting entity to determine if ecrit compatible emergency call support is available in the jurisdiction where the location is proffered for

mapping. Where ecrit compatible emergency calling is NOT available, the mapping function MAY yield information which could be used to route emergency calls using existing, country specific methods. For example, a tel URI may be provided for a PSTN routed call, or a routing code which has meaning only within a country specific routing mechanism.

I25. Mapping can be requested from anywhere: The mapping protocol MUST be able to provide the mapping regardless of where the querier is located, either geographically or by network location.

Motivation: The querier, such as the ESRP, may not necessarily be anywhere close to the caller or the appropriate PSAP, but must still be able to obtain a mapping.

I31: In response to a mapping request, a server will normally provide a URI or set of URIs for contacting the appropriate PSAP. The protocol must also be to return a URI or contact method explicitly marked as an alternate contact. When this is used will be described in an operational document.

I39: It SHOULD be possible to have updates of location (which may occur when measuring devices provider early, but imprecise "first fix" location) which can change routing of calls.

I40. The mapping protocol MUST be extensible to allow for the inclusion of new location fields.

Motivation: This is needed, for example, to accommodate future extensions to location information that might be included in the PIDF-LO.

I41. Split responsibility: The mapping protocol MUST allow that within a single level of the civic address hierarchy, multiple mapping servers handle subsets of the data elements.

Motivation: For example, two directories for the same city or county may handle different streets within that city or county.

I42. The mapping function MUST be able to be invoked at any time, including while an emergency call is in process.

7. Emergency Address Directory

- D1. PSAP Identification: The mapping information **MUST** be available without having to enroll with a service provider.

Motivation: The mapping server may well be operated by a service provider, but access to the server offering the mapping **MUST NOT** require use of a specific ISP or VSP.

- D5. Call setup latency: The directory lookup **SHOULD** minimize any added delay to the call setup.

Motivation: Since outbound proxies will likely be asked to resolve the same geographic coordinates repeatedly, a suitable time-limited caching mechanism should be supported.

- D7. Referral: The querier **MUST** be able to contact any server and be referred to another server that is more qualified to answer the query.

Motivation: This requirement alleviates the potential for misconfigurations to cause calls to fail, particularly for caller-based queries.

- D9. Baseline query protocol: A mandatory-to-implement protocol **MUST** be specified.

Motivation: An over-abundance of similarly-capable choices appears undesirable for interoperability.

Internet-Draft

ECRIT requirements

May 2005

[8.](#) Supplemental Information

SD1 The format both of the query and of the result returned by the protocol must be extensible to accommodate new types of information.

Motivation: In addition to information sent with the call, additional information may be available, supplemental to the call, which is retrieved from internal or external databases using a key to the information included with the call. This key may also include information to identify/address the database.

SD2 Additional information MAY be available to the call taker based on the location of the caller.

SD3 Additional information MAY be available to the call taker based on the owner of the structure.

SD4 Additional information MAY be available to the call taker based on the tenant of the structure.

SD5 Where a vehicle is involved, additional information MAY be available.

SD6 Additional information MAY be available based on the Address of Record (AoR) of the caller. In this context, AoR equates to the caller.

SD7 Consideration SHOULD be given to permitting users to have domain independent mechanisms to supply information related to the caller, for example, another datum related to user.

SD8. Additional Data: Transfer of additional data SHOULD be supported.

Motivation: Capabilities to contact PSAP by automatic means and for the transfer of additional information (alarm equipment, cars, buses, trucks with dangerous loads, ...)

SD9 Mechanism MUST be provided to automatically generate and provide

misroute and location error reports.

Schulzrinne & Marshall	Expires November 2, 2005	[Page 17]
------------------------	--------------------------	-----------

Internet-Draft	ECRIT requirements	May 2005
----------------	--------------------	----------

[9.](#) Security Considerations

Note: Security Considerations are referenced in the ECRIT security document [\[3\]](#).

10. Contributors

The information contained in this document is a result of a joint effort based on individual contributions by those involved in the ECRIT WG. The contributors include Nadine Abbott, Hideki Arai, Martin Dawson, Motoharu Kawanishi, Brian Rosen, Richard Stastny, Martin Thomson, James Winterbottom.

The contributors can be reached at:

Nadine Abbott	nabbott@telcordia.com
Hideki Arai	arai859@oki.com
Martin Dawson	mdawson@nortelnetworks.com
Motoharu Kawanishi	kawanishi381@oki.com
Brian Rosen	br@brianrosen.net
Richard Stastny	Richard.Stastny@oefeg.at
Martin Thomson	marthom@nortelnetworks.com
James Winterbottom	winterb@nortelnetworks.com

Schulzrinne & Marshall

Expires November 2, 2005

[Page 19]

Internet-Draft

ECRIT requirements

May 2005

[11.](#) Acknowledgments

[12.](#) References

[12.1](#) Normative References

- [1] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", [BCP 14](#), [RFC 2119](#), March 1997.
- [2] Polk, J., "Requirements for Session Initiation Protocol Location Conveyance", [draft-ietf-sipping-location-requirements-02](#) (work in progress), October 2004.
- [3] Tschofenig, H., "Security Threats and Requirements for Emergency

Calling", [draft-tschofenig-ecrit-security-threats-00](#) (work in progress), May 2005.

[12.2](#) Informative References

- [4] Charlton, N., Gasson, M., Gybels, G., Spanner, M., and A. van Wijk, "User Requirements for the Session Initiation Protocol (SIP) in Support of Deaf, Hard of Hearing and Speech-impaired Individuals", [RFC 3351](#), August 2002.
- [5] Cuellar, J., Morris, J., Mulligan, D., Peterson, J., and J. Polk, "Geopriv Requirements", [RFC 3693](#), February 2004.
- [6] National Emergency Number Association, "NENA technical information document on the interface between the E9-1-1 service providers network and the Internet protocol (IP) PSAP", NENA NENA-08-501, February 2003.

Authors' Addresses

Henning Schulzrinne
Columbia University
Department of Computer Science
450 Computer Science Building
New York, NY 10027
US

Phone: +1 212 939 7004
Email: hgs+ecrit@cs.columbia.edu
URI: <http://www.cs.columbia.edu>

Roger Marshall (editor)
TeleCommunication Systems
2401 Elliott Avenue
2nd Floor
Seattle, WA 98121

US

Phone: +1 206 792 2424

Email: rmarshall@telecomsys.com

URI: <http://www.telecomsys.com>

Intellectual Property Statement

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.

Disclaimer of Validity

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 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.

Copyright Statement

Copyright (C) The Internet Society (2005). 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.

Acknowledgment

Funding for the RFC Editor function is currently provided by the Internet Society.

