ECRIT	H. Schulzrinne
Internet-Draft	Columbia University
Intended status: Standards Track	S. McCann
Expires: January 12, 2012	Research in Motion UK Ltd
	G. Bajko
	Nokia
	H. Tschofenig
	Nokia Siemens Networks
	D. Kroeselberg
	Siemens
	July 11, 2011

Extensions to the Emergency Services Architecture for dealing with Unauthenticated and Unauthorized Devices

draft-ietf-ecrit-unauthenticated-access-03.txt

Abstract

The IETF emergency services architecture assumes that the calling device has acquired rights to use the access network or that no authentication is required for the access network, such as for public wireless access points. Subsequent protocol interactions, such as obtaining location information, learning the address of the Public Safety Answering Point (PSAP) and the emergency call itself are largely decoupled from the underlying network access procedures.

In some cases, however, the device does not have these credentials for network access, does not have a VoIP service provider, or the credentials have become invalid, e.g., because the user has exhausted their prepaid balance or the account has expired.

This document provides a problem statement, introduces terminology and describes an extension for the base IETF emergency services architecture to address these scenarios.

Status of this Memo

Copyright Notice

Table of Contents

1. Introduction

Summoning police, the fire department or an ambulance in emergencies is one of the fundamental and most-valued functions of the telephone. As telephone functionality moves from circuit-switched telephony to Internet telephony, its users rightfully expect that this core functionality will continue to work at least as well as it has for the older technology. New devices and services are being made available that could be used to make a request for help, which are not traditional telephones, and users are increasingly expecting them to be used to place emergency calls.

Roughly speaking, the IETF emergency services architecture (see [I-D.ietf-ecrit-phonebcp] and [I-D.ietf-ecrit-framework]) divides responsibility for handling emergency calls between the access network (ISP), the application service provider (ASP) that may be a VoIP service provider and the provider of emergency signaling services, the emergency service network (ESN). The access network may provide location information to end systems, but does not have to provide any ASP signaling functionality. The emergency caller can reach the ESN either directly or through the ASP's outbound proxy. Any of the three parties can provide the mapping from location to PSAP URI by offering LoST [RFC5222] services.

In general, a set of automated configuration mechanisms allows a device to function in a variety of architectures, without the user being aware of the details on who provides location, mapping services or call routing services. However, if emergency calling is to be supported when the calling device lacks access network authorization or does not have an ASP, one or more of the providers may need to provide additional services and functions.

In all cases, the end device has to be able to perform a LoST lookup and otherwise conduct the emergency call in the same manner as when the three exceptional conditions discussed below do not apply.

We distinguish between three conditions:

No Access Authentication (NAA): In the NAA case, the emergency caller does not posses valid credentials for the access network. This includes the case where the access network allows pay-per-use, as is common for wireless hotspots, but there is insufficient time to enter credit card details and other registration information required for access. It also covers all cases where either no credentials are available at all, or the available credentials do not work for the given IAP/ISP. As a result, the NAA case basically combines the below NASP and ZBP cases, but at the IAP/ISP level. Support for emergency call handling in the NAA case is subject to the local policy of the ISP. Such policy may vary substantially between ISPs and typically depends on external factors that are not under the ISP control.

No ASP (NASP): The caller does not have an ASP at the time of the call. This can occur either in case the caller does not possess any valid subscription for a reachable ASP, or in case none of the ASPs where the caller owns a valid subscription is reachable through the ISP.

Note: The interoperability need is increased with this scenario since the client software used by the emergency caller must be compatible with the protocols and extensions deployed by the ESN.

Zero-balance ASP (ZBP): In the case of zero-balance ASP, the ASP can authenticate the caller, but the caller is not authorized to use ASP services, e.g., because the contract has expired or the prepaid account for the customer has been depleted.

These three cases are not mutually exclusive. A caller in need for help may find himself/herself in, for example, a NAA and NASP situation, as explained in more details in Figure 1. Depending on local policy and regulations, it may not be possible to place emergency calls in the NAA case. Unless local regulations require user identification, it should always be possible to place calls in the NASP case, with minimal impact on the ISP. Unless the ESN requires that all calls traverse a known set of VSPs, it is technically possible to let a caller place an emergency call in the ZBP case. We discuss each case in more details in Section 3.

Note: At the time of writing there is no regulation in place that demands the functionality described in this memo. SDOs have started their work on this subject in a proactive fashion in the anticipation that national regulation will demand it for a subset of network environments.
There are also indications that the functionality of unauthenticated emergency calls (called SIM-less calls) in today's cellular system in certain countries leads to a fair amount of hoax or test calls. This causes overload situations at PSAPs which is considered harmful to the overall availability and reliability of emergency services.
As an example, Federal Office of Communications (OFCOM, Switzerland) provided statistics about emergency (112) calls in Switzerland from Jan. 1997 to Nov. 2001. Switzerland did not offer SIM-less emergency calls except for almost a month in July 2000 where a significant increase in hoax and test calls was reported. As a consequence, the functionality was disabled again. More details can be found in the panel presentations of the 3rd SDO Emergency Services Workshop [esw07].

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 [RFC2119].
This document reuses terminology from [RFC5687] and [RFC5012], namely Internet Access Provider (IAP), Internet Service Provider (ISP), Application Service Provider (ASP), Voice Service Provider (VSP), Emergency Service Routing Proxy (ESRP), Public Safety Answering Point (PSAP), Location Configuration Server (LCS), (emergency) service dial string, and (emergency) service identifier.

3. Use Case Categories

On a very high-level, the steps to be performed by an end host not being attached to the network and the user starting to make an emergency call are the following:

Link Layer Attachment: Some radio networks have added support for unauthenticated emergency access, some other type of networks advertise these capabilities using layer beacons. The end host learns about these unauthenticated emergency services capabilities either from the link layer type or from advertisement.

The end host uses the link layer specific network attachment procedures defined for unauthenticated network access in order to get access to the network.

Pre-Emergency Service Configuration: When the link layer network attachment procedure is completed the end host learns basic configuration information using DHCP from the ISP. The end host uses a Location Configuration Protocol (LCP) to retrieve location information. Subsequently, the LoST protocol [RFC5222] is used to learn the relevant emergency numbers, and to obtain the PSAP URI applicable for that location.

Emergency Call: In case of need for help, a user dials an emergency number and the SIP UA initiates the emergency call procedures by communicating with the PSAP.

Figure 1 compiles the basic logic taking place during network entry for requesting an emergency service and shows the interrelation between the three conditions described in the above section.

```
                         +-----Y
                         |Start|
                         `...../
                            |
                            | Are credentials
                            | for network attachment
                            | available?
                            |
               NO           v         YES
             +----------------------------+
             |                            |
             |                            |
             V                            v
        ..............               ................
        | Idle: Wait |               |Execute       |
        | for ES Call|               |LLA Procedures|
        | Initiation |               "--------------'
        "------------'                    |
    Is        |               +---------->O
    emergency |               |           | Is ASP
    service   | NO +-----Y    |           | configured?
    network   +--->| End |    |           +---------------+
    attachment|    `...../    |       YES |               | NO
    possible? |               |           |               |
              v               |           v               v
        +------------+        |     +------------+    +------------+
        | Execute    |        |     | Execute    |    | Execute    |
        | NAA        |--------+     | Phone BCP  |    | NASP       |
        | Procedures |              | Procedures |    | Procedures |
        +------------+              +------------+    +------------+
                         Authorization for|                 |
                         Emergency Call?  |                 |
                           +--------------+                 v
                           | NO           | YES         +-----Y
                           |              |             | Done|
                           v              v             `...../
                    +------------+  +------------+
                    | Execute    |  | Execute    |
                    | ZBP        |  | Phone BCP  |
                    | Procedures |  | Procedures |
                    +------------+  +------------+
                           |              |
                           |              |
                           v              v
                        +-----Y        +-----Y
                        | Done|        | Done|
                        `...../        `...../
```

Abbreviations:

LLA: Link Layer Attachment
ES: Emergency Services

4. ZBP Considerations

ZBP includes all cases where a subscriber is known to an ASP, but lacks the necessary authorization to access regular ASP services. Example ZBP cases include empty prepaid accounts, barred accounts, roaming and mobility restrictions, or any other conditions set by ASP policy. Local regulation might demand that emergency calls are always authorized. An ASP can identify emergency sessions by identifying the service URN [RFC5031] used in call setup. Emergency calls can then be authorized accordingly. The ZBP case therefore only affects the ASP. Permitting a call with limited authorization could present an opportunity for abuse. The ASP MAY choose to validate session initiation messages for valid destinations, see Section 7. An ASP without a regulatory requirement to authorize emergency calls can deny emergency call setup. Where an ASP does not authorize an emergency call, the caller can fall back to NASP procedures.

5. NASP Considerations

To start the description we consider the sequence of steps that are executed in an emergency call based on Figure 2.

- As an initial step the devices attaches to the network as shown in step (1). This step is outside the scope of this section.

- When the link layer network attachment procedure is completed the end host learns basic configuration information using DHCP from the ISP, as shown in step (2).

- When the IP address configuration is completed then the end host starts an interaction with the discovered Location Configuration Server at the ISP, as shown in step (3). The ISP may in certain deployments need to interact with the IAP. This protocol exchange is shown in step (4).

- Once location information is obtained the end host triggers the LoST protocol to obtain the address of the ESRP/PSAP. This step is shown in (5).

- In step (6), the SIP UA initiates a SIP INVITE towards the indicated ESRP. The INVITE message contains all the necessary parameters required by Section 5.1.5.

- The ESRP receives the INVITE and processes it according to the description in Section 5.3.3.

* The ESRP routes the call to the PSAP, as shown in (8), potentially interacting with a LoST server first to determine the route.

* The PSAP evaluates the initial INVITE and aims to complete the call setup.

* Finally, when the call setup is completed media traffic can be exchanged between the PSAP and the SIP UA.

For editorial reasons the end-to-end SIP and media exchange between the PSAP and SIP UA are not shown in Figure 2.

```
                               +-------+
                               | PSAP  |
                               |       |
                               +-------+
                                   ^
                                   | (8)
                                   |
            +----------+(7) +----------+
            | LoST     |<-->| ESRP     |
            | Server   |    |          |
            +----------+    +----------+
                  ^                ^
 +----------------+----------------|--------------+
 | ISP            |                |              |
 |+----------+    |                |  +----------+|
 || LCS-ISP  | (3)|                |  | DHCP     ||
 ||          |<-+ |                |  | Server   ||
 |+----------+  | |                |  +----------+|
 +-------^------+-+----------------|-----------^--+
 +-------|------+-+----------------|-----------|--+
 | IAP   | (4)  | |(5)             |           |  |
 |       V      | |                |           |  |
 |+----------+  | |                |           |  |
 || LCS-IAP  |  | |  +--------+    |           |  |
 ||          |  | |  | Link   |    |(6)        |  |
 |+----------+  | |  | Layer  |    |           |  |
 |              | |  | Device |    |        (2)|  |
 |              | |  +--------+    |           |  |
 |              | |      ^         |           |  |
 |              | |      |         |           |  |
 +--------------+-|-------|--------|-----------|--+
                | |       |        |           |
                | |    (1)|        |           |
                | |       |        |           |
                | |       |   +----+           |
                | |       v   |                |
                | |  +----------+              |
                | +->| End      |<-------------+
                +___>| Host     |
                     +----------+
```

Note: Figure 2 does not indicate who operates the ESRP and the LoST server. Various deployment options exist.

5.1. End Host Profile

5.1.1. LoST Server Discovery

The end host MUST discover a LoST server [RFC5222] using DHCP [RFC5223].

5.1.2. ESRP Discovery

The end host MUST discover the ESRP using the LoST protocol [RFC5222].

5.1.3. Location Determination and Location Configuration

The end host MUST support location acquisition and the LCPs described in Section 6.5 of [I-D.ietf-ecrit-phonebcp]. The description in Section 6.5 and 6.6 of [I-D.ietf-ecrit-phonebcp] regarding the interaction between the device and the LIS applies to this document.
The SIP UA in the end host MUST attach available location information in a PIDF-LO [RFC4119] when making an emergency call. When constructing the PIDF-LO the guidelines in PIDF-LO profile [RFC5491] MUST be followed. For civic location information the format defined in [RFC5139] MUST be supported.

5.1.4. Emergency Call Identification

To determine which calls are emergency calls, some entity needs to map a user entered dialstring into this URN scheme. A user may "dial" 1-1-2, but the call would be sent to urn:service:sos. This mapping SHOULD be performed at the endpoint device.
End hosts MUST use the Service URN mechanism [RFC5031] to mark calls as emergency calls for their home emergency dial string.

5.1.5. SIP Emergency Call Signaling

SIP signaling capabilities [RFC3261] are mandated for end hosts.
The initial SIP signaling method is an INVITE. The SIP INVITE request MUST be constructed according to the requirements in Section 9.2 [I-D.ietf-ecrit-phonebcp].
Regarding callback behavior SIP UAs SHOULD place a globally routable URI in a Contact: header.

5.1.6. Media

End points MUST comply with the media requirements for end points placing an emergency call found in Section 14 of [I-D.ietf-ecrit-phonebcp].

5.1.7. Testing

The description in Section 15 of [I-D.ietf-ecrit-phonebcp] is fully applicable to this document.

5.2. IAP/ISP Profile

5.2.1. ESRP Discovery

An ISP MUST provision a DHCP server with information about LoST servers [RFC5223]. An ISP operator may choose to deploy a LoST server or to outsource it to other parties.

5.2.2. Location Determination and Location Configuration

The ISP is responsible for location determination and exposes this information to the end points via location configuration protocols. The considerations described in [I-D.ietf-ecrit-location-hiding-req] are applicable to this document.
The ISP MUST support one of the LCPs described in Section 6.5 of [I-D.ietf-ecrit-phonebcp]. The description in Section 6.5 and 6.6 of [I-D.ietf-ecrit-phonebcp] regarding the interaction between the end device and the LIS applies to this document.
The interaction between the LIS at the ISP and the IAP is often priorietary but the description in [I-D.winterbottom-geopriv-lis2lis-req] may be relevant to the reader.

5.3. ESRP Profile

5.3.1. Emergency Call Routing

The ESRP continues to route the emergency call to the PSAP responsible for the physical location of the end host. This may require further interactions with LoST servers but depends on the specific deployment.

5.3.2. Emergency Call Identification

The ESRP MUST understand the Service URN mechanism [RFC5031] (i.e., the 'urn:service:sos' tree).

5.3.3. SIP Emergency Call Signaling

SIP signaling capabilities [RFC3261] are mandated for the ESRP. The ESRP MUST process the messages sent by the client, according to Section 5.1.5.

6. Lower Layer Considerations for NAA Case

Some radio networks have added support for unauthenticated emergency access, some other type of networks advertise these capabilities using layer beacons. The end host learns about these unauthenticated emergency services capabilities either from the link layer type or from advertisement.

This section discusses different methods to indicate an emergency service request as part of network attachment. It provides some general considerations and recommendations that are not specific to the access technology.

To perform network attachment and get access to the resources provided by an IAP/ISP, the end host uses access technology specific network attachment procedures, including for example network detection and selection, authentication, and authorization. For initial network attachment of an emergency service requester, the method of how the emergency indication is given to the IAP/ISP is specific to the access technology. However, a number of general approaches can be identified:

Link layer emergency indication: The end host provides an indication, e.g. an emergency parameter or flag, as part of the link layer signaling for initial network attachment. Examples include an emergency bit signalled in the IEEE 802.16-2009 wireless link. In IEEE 802.11 WLAN, an emergency support indicator allows the STA to download before association an NAI which it can use to request server side authentication only for an 802.1x network.

Higher-layer emergency indication: Typically emergency indication in access authentication. The emergency caller's end host provides an indication as part of the access authentication exchanges. EAP based authentication is of particular relevance here. Examples are the EAP NAI decoration used in WiMAX networks and modification of the authentication exchange in IEEE 802.11. [nwgstg3].

6.1. Link Layer Emergency Indication

In general, link layer emergency indications provide good integration into the actual network access procedure regarding the enabling of means to recognize and prioritize an emergency service request from an end host at a very early stage of the network attachment procedure. However, support in end hosts for such methods cannot be considered to be commonly available.

No general recommendations are given in the scope of this memo due to the following reasons:

- Dependency on the specific access technology.

- Dependency on the specific access network architecture. Access authorization and policy decisions typically happen at a different layers of the protocol stack and in different entities than those terminating the link-layer signaling. As a result, link layer indications need to be distributed and translated between the different involved protocol layers and entities. Appropriate methods are specific to the actual architecture of the IAP/ISP network.

* An advantage of combining emergency indications with the actual network attachment procedure performing authentication and authorization is the fact that the emergency indication can directly be taken into account in the authentication and authorization server that owns the policy for granting access to the network resources. As a result, there is no direct dependency on the access network architecture that otherwise would need to take care of merging link-layer indications into the AA and policy decision process.

* EAP signaling happens at a relatively early stage of network attachment, so it is likely to match most requirements for prioritization of emergency signaling. However, it does not cover early stages of link layer activity in the network attachment process. Possible conflicts may arise e.g. in case of MAC-based filtering in entities terminating the link-layer signaling in the network (like a base station). In normal operation, EAP related information will only be recognized in the NAS. Any entity residing between end host and NAS should not be expected to understand/parse EAP messages.

* An emergency indication can be given by forming a specific NAI that is used as the identity in EAP based authentication for network entry.

6.2. Securing Network Attachment in NAA Cases

For network attachment in NAA cases, it may make sense to secure the link-layer connection between the device and the IAP/ISP. This especially holds for wireless access with examples being IEEE 802.11 or IEEE 802.16 based access. The latter even mandates secured communication across the wireless link for all IAP/ISP networks based on [nwgstg3].
Therefore, for network attachment that is by default based on EAP authentication it is desirable also for NAA network attachment to use a key-generating EAP method (that provides an MSK key to the authenticator to bootstrap further key derivation for protecting the wireless link).
The following approaches to match the above can be identified:

1) Server-only Authentication:

The device of the emergency service requester performs an EAP method with the IAP/ISP EAP server that performs server side authentication only. An example for this is EAP-TLS. This provides a certain level of assurance about the IAP/ISP to the device user. It requires the device to be provisioned with appropriate trusted root certificates to be able to verify the server certificate of the EAP server (unless this step is explicitly skipped in the device in case of an emergency service request). This method is used to provide access of devices without existing credentials to an 802.1x network. The details are incorporated into the not yet published 802.11-2011 specification.

2) Null Authentication:

In one case (e.g. WiMAX) an EAP method is performed. However, no credentials specific to either the server or the device or subscription are used as part of the authentication exchange. An example for this would be an EAP-TLS exchange with using the TLS_DH_anon (anonymous) ciphersuite. Alternatively, a publicly available static key for emergency access could be used. In the latter case, the device would need to be provisioned with the appropriate emergency key for the IAP/ISP in advance. In another case (e.g. IEEE 802.11), no EAP method is used, so that empty frames are transported during the over the air IEEE 802.1X exchange. In this case the authentication state machine completes with no cryptographic keys being exchanged.

3) Device Authentication:

This case extends the server-only authentication case. If the device is configured with a device certificate and the IAP/ISP EAP server can rely on a trusted root allowing the EAP server to verify the device certificate, at least the device identity (e.g., the MAC address) can be authenticated by the IAP/ISP in NAA cases. An example for this are WiMAX devices that are shipped with device certificates issued under the global WiMAX device public-key infrastructure. To perform unauthenticated emergency calls, if allowed by the IAP/ISP, such devices perform EAP-TLS based network attachment with client authentication based on the device certificate.

7. Security Considerations

The security threats discussed in [RFC5069] are applicable to this document.
There are a couple of new vulnerabilities raised with unauthenticated emergency services in NASP/NAA cases since the PSAP operator will typically not possess any identity information about the emergency call via the signaling path itself. In countries where this functionality is used for GSM networks today this has lead to a significant amount of misuse.

In the context of NAA, the IAP and the ISP will probably want to make sure that the claimed emergency caller indeed performs an emergency call rather than using the network for other purposes, and thereby acting fraudulent by skipping any authentication, authorization and accounting procedures. By restricting access of the unauthenticated emergency caller to the LoST server and the PSAP URI, traffic can be restricted only to emergency calls. This can be accomplished with traffic separation. The details, however, e.g. for using filtering, depend on the deployed ISP architecture and are beyond the scope of this document.

We only illustrate a possible model. If the ISP runs its own LoST server, it would maintain an access control list including all IP addresses contained in responses returned by the LoST server, as well as the LoST server itself. (It may need to translate the domain names returned to IP addresses and hope that the resolution captures all possible DNS responses.) Since the media destination addresses are not predictable, the ISP also has to provide a SIP outbound proxy so that it can determine the media addresses and add those to the filter list.

For the ZBP case the additional aspect of fraud has to be considered. Unless the emergency call traverses a PSTN gateway or the ASP charges for IP-to-IP calls, there is little potential for fraud. If the ASP also operates the LoST server, the outbound proxy MAY restrict outbound calls to the SIP URIs returned by the LoST server. It is NOT RECOMMENDED to rely on a fixed list of SIP URIs, as that list may change.

Finally, a number of security vulnerabilities discussed in [I-D.ietf-geopriv-arch] around faked location information are less problematic in the context of unauthenticated emergency since location information does not need to be provided by the end host itself or it can be verified to fall within a specific geographical area.

8. Acknowledgments

Parts of this document are derived from [I-D.ietf-ecrit-phonebcp]. Participants of the 2nd and 3rd SDO Emergency Services Workshop provided helpful input.

We would like to thank Richard Barnes, Brian Rosen, James Polk, Marc Linsner, and Martin Thomson for their feedback at the IETF#80 ECRIT meeting.

Furthermore, we would like to thank Martin Thomson and Bernard Aboba for their detailed document review in preparation of the 81st IETF meeting.

9. IANA Considerations

This document does not require actions by IANA.

10. References

10.1. Normative References

[RFC5031]	Schulzrinne, H., "A Uniform Resource Name (URN) for Emergency and Other Well-Known Services", RFC 5031, January 2008.
[RFC4119]	Peterson, J., "A Presence-based GEOPRIV Location Object Format", RFC 4119, December 2005.
[RFC5491]	Winterbottom, J., Thomson, M. and H. Tschofenig, "GEOPRIV Presence Information Data Format Location Object (PIDF-LO) Usage Clarification, Considerations, and Recommendations", RFC 5491, March 2009.
[RFC5139]	Thomson, M. and J. Winterbottom, "Revised Civic Location Format for Presence Information Data Format Location Object (PIDF-LO)", RFC 5139, February 2008.
[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.
[RFC2119]	Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.
[I-D.ietf-ecrit-phonebcp]	Rosen, B and J Polk, "Best Current Practice for Communications Services in support of Emergency Calling", Internet-Draft draft-ietf-ecrit-phonebcp-20, September 2011.
[RFC5222]	Hardie, T., Newton, A., Schulzrinne, H. and H. Tschofenig, "LoST: A Location-to-Service Translation Protocol", RFC 5222, August 2008.
[RFC5223]	Schulzrinne, H., Polk, J. and H. Tschofenig, "Discovering Location-to-Service Translation (LoST) Servers Using the Dynamic Host Configuration Protocol (DHCP)", RFC 5223, August 2008.

10.2. Informative References

[RFC5687]	Tschofenig, H. and H. Schulzrinne, "GEOPRIV Layer 7 Location Configuration Protocol: Problem Statement and Requirements", RFC 5687, March 2010.
[I-D.ietf-ecrit-framework]	Rosen, B, Schulzrinne, H, Polk, J and A Newton, "Framework for Emergency Calling using Internet Multimedia", Internet-Draft draft-ietf-ecrit-framework-13, September 2011.
[I-D.ietf-geopriv-res-gw-lis-discovery]	Thomson, M and R Bellis, "Location Information Server (LIS) Discovery using IP address and Reverse DNS", Internet-Draft draft-ietf-

	geopriv-res-gw-lis-discovery-02, September 2011.
[RFC5985]	Barnes, M., "HTTP-Enabled Location Delivery (HELD)", RFC 5985, September 2010.
[RFC5012]	Schulzrinne, H. and R. Marshall, "Requirements for Emergency Context Resolution with Internet Technologies", RFC 5012, January 2008.
[I-D.ietf-ecrit-location-hiding-req]	Schulzrinne, H, Liess, L, Tschofenig, H, Stark, B and A Kuett, "Location Hiding: Problem Statement and Requirements", Internet-Draft draft-ietf-ecrit-location-hiding-req-04, February 2010.
[I-D.winterbottom-geopriv-lis2lis-req]	Winterbottom, J and S Norreys, "LIS to LIS Protocol Requirements", Internet-Draft draft-winterbottom-geopriv-lis2lis-req-01, November 2007.
[RFC5069]	Taylor, T., Tschofenig, H., Schulzrinne, H. and M. Shanmugam, "Security Threats and Requirements for Emergency Call Marking and Mapping", RFC 5069, January 2008.
[I-D.ietf-geopriv-arch]	Barnes, R, Lepinski, M, Cooper, A, Morris, J, Tschofenig, H and H Schulzrinne, "An Architecture for Location and Location Privacy in Internet Applications", Internet-Draft draft-ietf-geopriv-arch-03, October 2010.
[esw07]	, , "3rd SDO Emergency Services Workshop, http://www.emergency-services-coordination.info/2007Nov/", October 30th - November 1st 2007.
[nwgstg3]	, , "WiMAX Forum WMF-T33-001-R015V01, WiMAX Network Architecture Stage-3 http://www.wimaxforum.org/sites/wimaxforum.org/files/technical_document/2009/09/DRAFT-T33-001-R015v01-O_Network-Stage3-Base.pdf", September 2009.

Authors' Addresses

Henning Schulzrinne 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

Stephen McCann McCann Research in Motion UK Ltd 200 Bath Road Slough, Berks SL1 3XE UK Phone: +44 1753 667099 EMail: smccann@rim.com URI: http://www.rim.com

Gabor Bajko Bajko Nokia EMail: Gabor.Bajko@nokia.com

Hannes Tschofenig Tschofenig Nokia Siemens Networks Linnoitustie 6 Espoo, 02600 Finland Phone: +358 (50) 4871445 EMail: Hannes.Tschofenig@gmx.net URI: http://www.tschofenig.priv.at

Dirk Kroeselberg Kroeselberg Siemens Germany EMail: dirk.kroeselberg@siemens.com