Network Working Group
INTERNET-DRAFT
Category: Informational
Expires: December 30, 2012

B. Aboba
M. Thomson
Microsoft Corporation

30 June 2012

Emergency Services Support in WebRTC
draft-aboba-rtcweb-ecrit-00.txt

Abstract

The Web Real-Time Communication (WebRTC) framework supports interactive communication between web-browsers, including support for audio, video and text. This document describes how emergency services functionality can be implemented within the WebRTC framework, including support for location and call routing as well as interoperability with Public Safety Answering Points (PSAPs) supporting next generation emergency services.

Legal

THIS DOCUMENT AND THE INFORMATION CONTAINED THEREIN 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 THEREIN WILL NOT INFRINGE ANY RIGHTS OR ANY IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE.

Status of This Memo

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at http://datatracker.ietf.org/drafts/current/.

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."

This Internet-Draft will expire on December 30, 2012.

Copyright Notice

Copyright (c) 2012 IETF Trust and the persons identified as the document authors. All rights reserved.

This document is subject to BCP 78 and the IETF Trust's Legal Provisions Relating to IETF Documents (http://trustee.ietf.org/license-info) in effect on the date of publication of this document. Please review these documents carefully, as they describe your rights and restrictions with respect to this document. Code Components extracted from this document must include Simplified BSD License text as described in Section 4.e of the Trust Legal Provisions and are provided without warranty as described in the Simplified BSD License.

Table of Contents

1. Introduction 3
1.1 Terminology 3
1.2 Prior Work 4
2. Location and Call Routing Requirements 4
3 Media Requirements 7
4. Accessibility 8
5. Security Considerations 9
6. IANA Considerations 11
7. Acknowledgments 11
8. References 11
8.1. Normative References 11
8.2 Informative references 11
Authors' Addresses 15

1. Introduction

The Web Real-Time Communication (WebRTC) framework supports interactive communication between web-browsers, including support for audio, video and text. This document describes how emergency services functionality can be implemented within the WebRTC framework. Since signaling is out of scope of the WebRTC standards suite as noted in "Overview: Real Time Protocols for Browser-based Applications" [I-D.ietf-rtcweb-overview] Section 3, this document focuses on other aspects such as location, call routing and media support.

No guidance is provided as to whether a given WebRTC application or service will be subject to emergency service obligations. As noted in "Best Current Practice for Communications Services in support of Emergency Calling" [I-D.ietf-ecrit-phonebcp] Section 4:

> Some jurisdictions have regulations governing which devices need to support emergency calling and developers are encouraged to ensure that devices they develop meet relevant regulatory requirements. Unfortunately, the natural variation in those regulations also makes it impossible to accurately describe the cases when developers do or do not have to support emergency calling.

It should also be understood that this document does not advocate use of IP-based communication in all situations. For example, where accurate location cannot be obtained, emergency callers could be better served by utilizing the telephony capabilities of the underlying platform (e.g., a mobile-device) where available, as proposed in [WebTel]. This can enable location to be provided in situations where it would not otherwise be available, as well as permitting an emergency call to be placed even when the device does not have access to the Internet.

The document is laid out as follows: Section 1 provides an introduction and reviews prior work. Section 2 discusses requirements relating to location and call routing. Section 3 discusses media requirements. Section 4 discusses accessibility. Section 5 discusses security considerations.

1.1. 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].

This document uses terms from [RFC3261], [RFC5012] and [RFC6443].

1.2. Prior Work

The IETF ECRIT WG has developed an overview of the emergency calling architecture as well as a best current practice document detailing implementation requirements.

"Framework for Emergency Calling using Internet Multimedia" [RFC6443] provides an overview of how IETF specifications can be used to support emergency calling using multimedia. At a high level, this involves determination of the caller location, conveyance of the location within a signaling protocol such as Session Initiation Protocol (SIP) [RFC6442], routing of the call using the Location-to-Service Translation (LoST) protocol [RFC5222], and exchange of media using Real-time Transport Protocol (RTP) [RFC3550].

"Best Current Practice for Communication Services in support of Emergency Calling" [I-D.ietf-ecrit-phonebcp] builds on [RFC6443] to describe the requirements for end devices ("ED-" requirements), access networks ("AN-"), service providers ("SP-"), Public Safety Answering Points (PSAPs) and intermediate devices ("INT-") to achieve globally interoperable emergency calling on the Internet.

Both [RFC6443] and [I-D.ietf-ecrit-phonebcp] assume the use of SIP as the signaling mechanism for emergency calling. As noted in [RFC6443] Section 1:

> This document discusses the use of the Session Initiation Protocol (SIP) [RFC3261] by PSAPs and calling parties. While other inter-domain call signaling protocols may be used for emergency calling, SIP is ubiquitous and possesses the proper support of this use case.

Since standardization of signaling is out of scope of the WebRTC standards effort, and WebRTC applications can utilize a wide variety of signaling mechanisms, the requirements described in [I-D.ietf-ecrit-phonebcp] do not necessarily apply to WebRTC implementations, applications and services. Therefore in this document, we focus on emergency calling requirements that are independent of the signaling mechanism, such as those relating to accessibility, location, call routing and media.

2. Location and Call Routing Requirements

Determination of caller location as well as call routing is an essential aspect of emergency services support. Relevant requirements from [I-D.ietf-ecrit-phonebcp] include:

> ED-15/INT-4/AN-4 Devices, intermediate Devices and/or access

networks SHOULD support a manual method to override the location the access network determines. When the override location is supplied in civic form, it MUST be possible for the resultant Presence Information Data Format - Location Object (PIDF-LO) received at the PSAP to contain any of the elements specified in [RFC4119] and [RFC5139].

ED-17/INT-9/AN-9 Devices that support endpoint measuring of location MUST have at least a coarse location capability (typically <1km accuracy) for routing of calls. The location mechanism MAY be a service provided by the access network.

ED-24 Where the operating system supporting application programs which need location for emergency calls does not allow access to Layer 2 and Layer 3 functions necessary for a client application to use DHCP location options and/or other location technologies that are specific to the type of access network, the operating system MUST provide a published API conforming to ED-12 through ED-23 and ED-25 through ED-32. It is RECOMMENDED that all operating systems provide such an API.

ED-41/SP-20 Location objects MUST be created with information about the method by which the location was determined, such as GPS, manually entered, or based on access network topology included in a PIDF- LO "method" element. In addition, the source of the location information MUST be included in a PIDF-LO "provided-by" element.

ED-49 Endpoints MUST support one or more mechanisms that allow them to determine their public IP address, for example, STUN [RFC5389].

ED-50 Endpoints MUST support LIS discovery as described in [RFC5986], and the LoST discovery as described in [RFC5223].

Since browser applications do not have direct access to operating system location APIs, ED-24 is not applicable to WebRTC.

For reasons that will be described, automatically obtaining location suitable for emergency use is challenging for WebRTC applications. In order to ensure that location is available when needed, as well as to provide resilience against errors in automated location determination, WebRTC emergency service applications SHOULD support manual override as recommended in ED-15.

The W3C Geolocation API [GeolocationAPI] was not developed with emergency services location in mind, so that requirements ED-17 and ED-41 are not well supported. [GeolocationAPI] does not provide

information on the source of the location information as required in ED-41; attempting to infer the source from the accuracy parameter is NOT RECOMMENDED. Currently, Location Based Services utilized by Geolocation APIs do not warrant their use in emergency services and do not consistently provide the accuracy required by emergency services applications, so that emergency use of the W3C Geolocation API is also NOT RECOMMENDED.

An alternative is to implement location configuration and call routing in Javascript, using an HTTP-based protocol such as HELD [RFC5985] and LoST [RFC5222]. While this approach can provide location usable in emergency services applications, it is only applicable on networks with a Location Information Server (LIS), such as enterprise deployments subject to Multi-Line Telephone System (MLTS) regulations [StateMLTS].

In order to utilize location and call routing services, it is first necessary to locate the appropriate servers. Since the discovery mechanisms described in [RFC5986] and [RFC5223] are based on use of a DHCP option, which cannot be assumed to be accessible in Javascript, ED-50 is difficult to support within WebRTC-based emergency services applications.

For LoST discovery, the emergency services application can determine the appropriate LoST server(s) on its own. To avoid potential issues, it is best to avoid pre-configuration of particular servers, allowing the appropriate server to be determined dynamically.

LIS discovery requires determination of the domain name that can be used for LIS discovery, as noted in [RFC5986] Section 3.4:

> If a Device knows one or more alternative domain names that might be used for discovery, it MAY repeat the U-NAPTR process using those domain names as input. For instance, static configuration of a Device might be used to provide a Device with a domain name.

While static configuration of the domain name can be used in situations where device mobility is restricted, the appropriate LIS depends on the network to which the host is attached, so that this is not a general solution.

"Location Information Server (LIS) Discovery using IP address and Reverse DNS" [I.D.ietf-geopriv-res-gw-lis-discovery] specifies a means for a device to discover several alternative domain names that can be used as input to the Dynamic Delegation Discovery Service (DDDS). Since several of the techniques (such as use of PTR RRs and Session Traversal Utilities for NAT (STUN) [RFC5389]) are potentially implementable in WebRTC-based emergency services applications this

approach MAY be used.

3. Media Requirements

Within [I-D.ietf-ecrit-phonebcp] media-related requirements are covered in Section 14. These include:

> ED-71 Endpoints MUST send and receive media streams on RTP [RFC3550].
>
> ED-72 Normal SIP offer/answer [RFC3264] negotiations MUST be used to agree on the media streams to be used.
>
> ED-73/SP-41 G.711 A law (and mu Law if they are intended be used in North America) encoded voice as described in [RFC3551] MUST be supported. If the endpoint cannot support G.711, a transcoder MUST be used so that the offer received at the PSAP contains G.711. It is desirable to include wideband codecs such as G.722 and AMR-WB in the offer. PSAPs SHOULD support narrowband codecs common on endpoints in their area to avoid transcoding.
>
> ED-74 Silence suppression (Voice Activity Detection methods) MUST NOT be used on emergency calls. PSAP call takers sometimes get information on what is happening in the background to determine how to process the call.
>
> ED-77 Endpoints supporting video MUST support H.264 per [RFC6184].

Requirement ED-71 is satisfied by compliant WebRTC implementations since "Web Real-Time Communication (WebRTC): Media Transport and Use of RTP" [I-D.ietf-rtcweb-rtp-usage] Section 4.1 requires support for RTP [RFC3550].

Requirement ED-72 is specific to SIP and so does not apply generally to WebRTC implementations, applications and services. However, it is believed that the APIs under development within the W3C WebRTC WG can support this requirement.

Requirement ED-74 is satisfied by compliant WebRTC implementations since the WebRTC APIs under development within W3C [WEBRTC], support silence suppression control via the "constraints" parameter.

[I.D.ietf-rtcweb-rtp-usage] Section 4.3 does not provide a recommendation on a mandatory-to-implement set of codecs. While ED-73 does not require implementation of G.711 if the service supports transcoding, G.711 is not difficult to implement and is widely supported, with a high level of interoperability. Therefore it is recommended that G.711 be included as a mandatory-to-implement

audio codec within [I-D.ietf-rtcweb-rtp-usage] Section 4.3.

Currently the disposition of ED-77 is unclear. Discussion of mandatory-to-implement video codecs is ongoing within the IETF RTCWEB WG, but has not reached a conclusion. While there is a need to support interoperable video within emergency services applications, more options may be available within an emergency services context than would be the case for general use. For example, within the PSAP, it may be feasible to support multiple video codecs, either by installation of browser plugins, or by use of multiple browsers. In some emergency service applications (such as the VRS), codec requirements may be specific to the service and may be satisfiable by a custom device or browser approved for use with that service, which may include the required codecs implemented natively or via plug-ins, as the service provider sees fit.

4. Accessibility

By lowering the barriers to development of realtime-enabled browser applications, as well as by building on accessibility support within the browser, WebRTC promises to enable the development of a new generation of accessible emergency applications and services.

In order to support accessibility, it is RECOMMENDED that WebRTC-based emergency applications and services conform to the Web Content Accessibility Guidelines (WCAG) v2.0 [WCAG].

In order to support accessibility for individuals with hearing or speech disabilities, support for textual communications is important.

Currently the W3C is developing a proposed charter for the Timed Text Working Group [TTWG], which will potentially produce a second edition of the timed Text Markup Language (TTML) 1.0 recommendation as well as publishing a recommendation for a version 1.1 specification.

Text-related requirements in [I-D.ietf-ecrit-phonebcp] are covered in Section 14, including:

> ED-75 Endpoints supporting Instant Messaging (IM) MUST support either [RFC3428] and [RFC4975].
>
> ED-76 Endpoints supporting real-time text MUST use [RFC4103]. The expectations for emergency service support for the real-time text medium are described in [RFC5194], Section 7.1.

Since [RFC3428] and [RFC4975] are both based on SIP, ED-75 does not apply to all WebRTC-based emergency applications and services. As noted in "Emergency Services Functionality with the Extensible

Messaging and Presence Protocol (XMPP)" [I-D.tschofenig-ecrit-xmpp-es], XMPP [RFC6120] is a potential alternative for emergency services applications looking to support instant messaging [RFC6121] and multi-user chat [XEP-045] functionality.

"RTP Payload for Text Conversation" [RFC4103] is typically implemented along with SIP signaling as described in "Framework for Real-Time Text over IP Using the Session Initiation Protocol (SIP)" [RFC5194]. As a result, ED-76 does not apply to WebRTC implementations.

Alternatives to support of real-time text functionality are available, such as "In-Band Real Time Text" [XEP-0301], which supports real-time text by addition of child elements within XMPP message stanzas. The use of child elements to encapsulate real-time text, as well as transmission of complete lines enables [XEP-0301] to provide backward compatibility with existing XMPP instant-messaging and Multi-User Chat (MUC) clients, with no changes required to XMPP servers. Since XMPP can be encapsulated within HTTP via mechanisms such as BOSH [XEP-0206] or WebSockets [RFC6455], [XEP-0301] can be implemented in Javascript. Experience with Javascript implementation using the [Strophe] XMPP library indicates that adequate performance is achievable. In contrast, implementing real-time text as media as in [RFC4103] requires native browser support, as well as requiring changes to the configuration of intermediaries such as Session Border Controllers (SBCs). Also, [RFC4103] is not backward compatible with SIP instant messaging implementations supporting page-mode [RFC3428] or session [RFC4975] approaches.

5. Security Considerations

Security requirements in [I-D.ietf-ecrit-phonebcp] include:

ED-48/SP-24 TLS [RFC5746] MUST be used to protect location (but see Section 9.1). All implementations MUST support TLS.

ED-58/SP-30 TLS is the primary mechanism used to secure the signaling for emergency calls. IPsec [RFC4301] MAY be used instead of TLS for any hop. Either TLS or IPSEC MUST be used when attempting to signal an emergency call.

ED-59/SP-31 If TLS session establishment is not available, or fails, the call MUST be retried without TLS.

ED-60/SP-32 [RFC5626] is RECOMMENDED to maintain persistent TLS connections between entities when one of the entity is an endpoint. Persistent TLS connection between proxies is RECOMMENDED using any suitable mechanism.

> ED-61/AN-28 TLS SHOULD be used when attempting to retrieve location (configuration or dereferencing) with HELD. The use of [RFC5077] is RECOMMENDED to minimize the time to establish TLS sessions without keeping server-side state. IPsec MAY be used instead of TLS.
>
> ED-62/AN-29 When TLS session establishment fails, the location retrieval MUST be retried without TLS.

For WebRTC, HTTPS MUST be used to protect signaling for an emergency call, with potential fail-over to HTTP. HTTPS SHOULD be used to protect location retrieval (HELD) and call routing (LoST).

WebRTC security considerations are discussed in "Security Considerations for RTC-Web" [I-D.ietf-rtcweb-security]. The WebRTC security architecture, described in "RTCWEB Security Architecture" [I-D.ietf-rtcweb-security-arch], requires implementation of Secure RTP [RFC3711] as well as DTLS/SRTP [RFC5764].

While the security features of WebRTC exceed the requirements outlined in [I-D.ietf-ecrit-phonebcp], support for emergency services within WebRTC raises concerns about potential attacks on the emergency services infrastructure, given the potential for malicious code to be executed within the browser. One way to lessen the likelihood of attacks by untrusted Javascript applications is for PSAPs to put up their own sites for emergency calling, protected by HTTPS.

While ICE [RFC5245] provides demonstration of liveness and consent to receive, it is possible for an attacker to overwhelm the PSAP by generating a large number of prank calls. IP relay services are also potential targets since these don't require forging of Caller-Id nor do they provide audio or video from the attacker.

Security threats to IP-based emergency services are described in "Security Threats and Requirements for Emergency Call Marking and Mapping" [RFC5069]. These include attacks on the emergency services system, such as attempting to deny system services to all users in a given area, to gain fraudulent use of services and to divert emergency calls to non-emergency sites. [RFC5069] also describes attacks against individuals, including attempts to prevent an individual from receiving aid, or to gain information about an emergency.

"Threat Analysis of the Geopriv Protocol" [RFC3694] describes threats against geographic location privacy, including protocol threats, threats resulting from the storage of geographic location data, and threats posed by the abuse of information.

Overall, experience indicates a relationship between anonymity and the prevalence of prank calling. Therefore some protection may be provided through authentication of the caller either in the signaling or media plane. It is NOT RECOMMENDED that WebRTC-based emergency applications and services support anonymous emergency calling.

6. IANA Considerations

This document does not require actions by IANA.

7. Acknowledgments

We would like to thank the members of the IETF RTCWEB Working Group for discussions related to this topic.

8. References

8.1. Normative References

[I-D.ietf-ecrit-phonebcp]
Rosen, B. and J. Polk, "Best Current Practice for Communications Services in support of Emergency Calling", draft-ietf-ecrit-phonebcp-20 (work in progress), September 2011.

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

[WCAG] Caldwell, B., Cooper, M., Reid, L.G. and G. Vanderheiden, "Web Content Accessibility Guidelines (WCAG) 2.0", http://www.w3.org/TR/WCAG20/, December 2008.

8.2. Informative References

[GeolocationAPI]
Popescu, A., "Geolocation API Specification", W3C, http://dev.w3.org/geo/api/spec-source.html

[I.D.ietf-geopriv-res-gw-lis-discovery]
Thomson, M. and R. Bellis, "Location Information Server (LIS) Discovery using IP address and Reverse DNS", draft-ietf-geopriv-res-gw-lis-discovery-03 (work in progress), March 2012.

[I-D.ietf-rtcweb-overview]
Alvestrand, H., "Overview: Real Time Protocols for Browser-based Applications", draft-ietf-rtcweb-overview-04 (work in progress), June 2012.

[I-D.ietf-rtcweb-rtp-usage]
Perkins, C., Westerlund, M. and J. Ott, "Web Real-Time Communication (WebRTC): Media Transport and Use of RTP", draft-ietf-rtcweb-rtp-usage-03 (work in progress), June 2012.

[I-D.ietf-rtcweb-security]
Rescorla, E., "Security Considerations for RTC-Web", draft-ietf-rtcweb-security-03 (work in progress), June 2012.

[I-D.ietf-rtcweb-security-arch]
Rescorla, E., "RTCWEB Security Architecture", draft-ietf-rtcweb-security-arch-02 (work in progress), June 2012.

[I-D.tschofenig-ecrit-xmpp-es]
Tschofenig. H., "Emergency Services Functionality with the Extensible Messaging and Presence Protocol (XMPP)", draft-tschofenig-ecrit-xmpp-es-00 (work in progress), March 2012.

[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.

[RFC3264] Rosenberg, J. and R. Schulzrinne, "An Offer/Answer Model with the Session Description Protocol (SDP)", RFC 3264, June 2002.

[RFC3428] Campbell, B., Rosenberg, J., Schulzrinne, H., Huitema, C. and D. Gurle, "Session Initiation Protocol (SIP) Extension for Instant Messaging", RFC 3428, December 2002.

[RFC3550] Schulzrinne, H., Casner, S., Frederick, R., and V. Jacobson, "RTP: A Transport Protocol for Real-Time Applications", STD 64, RFC 3550, July 2003.

[RFC3551] Schulzrinne, H. and S. Casner, "RTP Profile for Audio and Video Conferences with Minimal Control", STD 65, RFC 3551, July 2003.

[RFC3694] Danley, M., Mulligan, D., Morris, J. and J. Peterson, "Threat Analysis of the Geopriv Protocol", RFC 3694, February 2004.

[RFC3711] Baugher, M., McGrew, D., Naslund, M., Carrara, E. and K. Norrman, "The Secure Real-time Transport Protocol (SRTP)", RFC 3711, March 2004.

[RFC4103] Hellstrom, G. and P. Jones, "RTP Payload for Text Conversation", RFC 4103, June 2005.

[RFC4119] Peterson, J., "A Presence-based GEOPRIV Location Object Format", RFC 4119, December 2005.

[RFC4301] Kent, S. and K. Seo, "Security Architecture for the Internet Protocol", RFC 4301, December 2005.

[RFC4975] Campbell, B., Mahy, R. and C. Jennings, "The Message Session Relay Protocol (MSRP)", RFC 4975, September 2007.

[RFC5012] Schulzrinne, H. and R. Marshall, "Requirements for Emergency Context Resolution with Internet Technologies", RFC 5012, January 2008.

[RFC5069] Taylor, T., Tschofenig, H., Schulzrinne, H. and M. Shanmugam, "Security Trheats and Requirements for Emergency Call Marking and Mapping", RFC 5069, January 2008.

[RFC5077] Salowey, J., Zhou, H., Eronen, P. and H. Tschofenig, "Transport Layer Security (TLS) Session Resumption without Server-Side State", RFC 5077, January 2008.

[RFC5139] Thomson, M. and J. Winterbottom, "Revised Civic Location Format for Presence Information Data Format Location Object (PIDF-LO)", RFC 5139, February 2008.

[RFC5194] van Wijk, A. and G. Gybels, "Framework for Real-Time Text over IP Using the Session Initiation Protocol (SIP)", RFC 5194, June 2008.

[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.

[RFC5245] Rosenberg, J., "Interactive Connectivity Establishment (ICE): A Protocol for Network Address Translator (NAT) Traversal for Offer/Answer Protocols", RFC 5245, April 2010.

[RFC5389] Rosenberg, J., Mahy, R., Matthews, P., and D. Wing, "Session Traversal Utilities for NAT", RFC 5389, October 2008.

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

[RFC5746] Rescorla, E., Ray, M., Dispensa, S. and N. Oskov, "Transport Layer Security (TLS) Renegotiation Indication Extension", RFC 5746, February 2010.

[RFC5764] McGrew, D. and E. Rescorla, "Datagram Transport Layer Security (DTLS) Extension to Establish Keys for the Secure Real-time Transport Protocol (SRTP)", RFC 5764, May 2010.

[RFC5985] Barnes, M., "HTTP Enabled Location Delivery (HELD)", RFC 5985, September 2010.

[RFC5986] Thomson, M. and J. Winterbottom, "Discovering the Local Location Information Server (LIS)", RFC 5986, September 2010.

[RFC6120] Saint-Andre, P., "Extensible Messaging and Presence Protocol (XMPP): Core", RFC 6120, March 2011.

[RFC6121] Saint-Andre, P., "Extensible Messaging and Presence Protocol (XMPP): Instant Messaging and Presence", RFC 6121, March 2011.

[RFC6184] Wang, Y.-K., Even, R., Kristensen, T. and R. Jesup, "RTP Payload Format for H.264 Video", RFC 6184, May 2011.

[RFC6442] Polk, J., Rosen, B. and J. Peterson, "Location Conveyance for the Session Initiation Protocol", RFC 6442, December 2011.

[RFC6443] Rosen, B., Schulzrinne. H., Polk, J. and A. Newton, "Framework for Emergency Calling Using Internet Multimedia", RFC 6443, December 2011.

[RFC6455] Fette, I. and A. Melnikov, "The WebSocket Protocol", RFC 6455, December 2011.

[StateMLTS] "State E911 Legislation", http://www1.911enable.com/resource-center/state-e911-legislation

[Strophe] "Libraries for XMPP Poets", http://strophe.im

[TTWG] "Proposed Timed Text Working Group Charter", http://www.w3.org/2012/02/timed-text-wg-charter.html

[WEBRTC] Bergkvist, A., Burnett, D., Jennings, C. and A. Narayanan, "WebRTC 1.0: Real-time Communication Between Browsers", W3C Editor's Draft (work in progress), http://dev.w3.org/2011/webrtc/editor/webrtc.html, May 2012.

[WebTel] WebAPI/WebTelephony, https://wiki.mozilla.org/WebAPI/WebTelephony

[XEP-0206] Paterson, I. and P. Saint-Andre, "XMPP Over BOSH", XEP-0206 version 1.3, http://xmpp.org/extensions/xep-0206.html, July 2010.

[XEP-0301] Rejhon, M., "In-Band Real Time Text", XEP-0301 version 0.2, http://xmpp.org/extensions/xep-0301.html, March 2012.

[XEP-045] Saint-Andre, P., "Multi-User Chat", XEP 0045 version 1.25, http://xmpp.org/extensions/xep-0045.html, February 2012.

Authors' Addresses

Bernard Aboba
Microsoft Corporation
One Microsoft Way
Redmond, WA 98052
US

EMail: bernard_aboba@hotmail.com

Martin Thomson
Skype
3210 Porter Drive
Palo Alto, CA 94304
US

Phone: +1 650-353-1925
Email: martin.thomson@gmail.com