ECRIT
Internet-Draft
Intended status: Informational
Expires: January 13, 2009

S. Norreys
BT Group
H. Tschofenig
Nokia Siemens Networks
H. Schulzrinne
Columbia University
July 12, 2008

Requirements for Authority-to-Individuals Communication for Emergency Situations
draft-norreys-ecrit-authority2individuals-requirements-01.txt

Status of this Memo

This Internet-Draft will expire on January 13, 2009.

Abstract

Public safety agencies need to provide information to the general public before and during large-scale emergencies. While many aspects of such systems are specific to national or local jurisdictions, emergencies span such boundaries and notifications need to reach visitors from other jurisdictions. This document summarizes requirements for protocols to alert individuals within a defined geographic area.

Table of Contents

1. Introduction

During large-scale emergencies, public safety authorities need to reliably communicate with citizens in the affected areas, to provide warnings, indicate whether citizens should evacuate and how, and to dispel misinformation. Accurate information can reduce the impact of such emergencies.

Traditionally, emergency alerting has used church bells, sirens, loudspeakers, radio and television to warn citizens and to provide information. However, techniques such as sirens and bells provide limited information content; loud speakers cover only very small areas and are often hard to understand, even for those not hearing impaired or fluent in the local language. Radio and television offer larger information volume, but are hard to target geographically and do not work well to address the "walking wounded" or other pedestrians. Both are not suitable for warnings, as many of those needing the information will not be listening or watching at any given time, particularly during work/school and sleep hours.

This problem has recently been illustrated by the London underground bombing on July 7, 2006, as described in a government report [ref]. The UK authorities could only use broadcast media and could not, for example, easily announce to the "walking wounded" where to assemble.

This document summarizes key requirements for IP-based protocols to enhance and complement existing authority-to-citizen warning systems. These protocols may either directly reach the citizen or may be used to trigger more traditional alerts, such as, among many others, displays in subway stations, electronic bill boards, or SMS.

Public safety authorities need to reach, with an appropriate message, as many affected people as possible within the area impacted by the emergency, including not just residents, but also workers and travelers who may only be in the area temporarily.

In addition, people around the immediately affected area should be able to receive information and differentiated instructions, such as warnings to avoid travel or to clear roads.

Emergency alerts may be issued once for an emergency or authorities may repeat or update information during an event.

Some messages are addressed to all individuals within a certain geographic area. Other messages may target only specific individuals or groups of individuals, such as medical personnel or those particularly susceptible to an incident.

Machine-parseable alerts may also be used to trigger automated behaviors, such as closing vents during a chemical spill or activating sirens or other warning systems in commercial buildings.

At least initially, mobile and stationary devices may not have the appropriate capabilities to receive such warnings. Thus, protocols need to be designed to allow gatewaying to traditional systems, e.g., the PSTN.

We assume an event notification model, i.e., individuals subscribe to warnings that affect their current location. As a mobile device moves, the subscription may need to be updated. Thus, location information needs to be available during the subscription process.

Users may want to subscribe to warnings that do not affect their current location. For example, parents may want to be alerted of emergencies affecting the school attended by their children and adult children may need to know about emergencies affecting elderly parents.

Some technologies may also support network-level broadcast or multicast.

2. Terminology

The keywords "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], with the

important qualification that, unless otherwise stated, these terms apply to the design of a protocol conveying emergency alerts and early warning messages, not its implementation or application.

This document reuses the terminology introduced by [3GPP-TR-22.968] and modifies it to fit to IETF terminology:

Notification Area:

Notification area is an area where warning notifications are sent.

Public Warning System:

A public warning system delivers warning notifications provided by warning notification providers to IP-capable end hosts within notification areas.

Warning Notification:

Warning notifications notify recipients of the occurrence of current or pending public safety-related events and additionally may provide users with instructions on what to do and where to get help for the duration of the emergency.

Warning Notification Provider:

A warning notification provider is an agency such as a branch of government or a public transport agency that provides warning notifications. A private institution, such as a university, hospital or enterprise, may also provide such warnings to people located within their facilities.

3. Requirements

The objective of these requirements is to allow authorities dealing with an emergency situation to communicate adequately with effected people in a timely fashion.

Req-1:

The protocol mechanisms MUST provide real-time message delivery.

Req-2:

The protocol mechanisms MUST deliver messages within a pre-planned time frame in the future, as agencies may want to prepare announcements for predictable or likely events.

Req-3:

The protocol mechanisms MUST convey sufficient details of the emergency situation.

Req-4:

The protocol mechanisms MUST provide the public with sufficient instructions to take appropriate actions.

Req-5:

The protocol mechanisms MUST allow targeting notifications to specific individuals, groups of individuals or specific geographic regions. Different regions or groups may receive different instructions for the same emergency. (For example, people very

close to a chemical spill may be asked to evacuate, while those further away may be asked to close windows.)

Req-6

Early warning notifications MAY be given preferential processing and delivery treatment.

Req-7

The protocol mechanisms MUST allow delivery of messages simultaneously to a large audience.

Req-8

The protocol mechanisms MAY provide an option to return a receipt on reading message. Message alert confirmation SHOULD NOT be required.

Req-9:

An emergency notification system MUST be independent of the underlying access network technology.

Req-10:

Protocol mechanisms MUST allow to tailor the message to the language preferences of the receiver and/or deliver multiple versions in different languages within the same message, so that the recipient can choose the most appropriate one.

Req-11:

A solution MUST support delivery of notification messages (e.g., with different media types) to those with special needs, such as hearing and vision impaired.

Req-12:

A user SHOULD be able to indicate the preferred method of communication to the public warning service, such as notification by email, different instant messaging protocols or automated voice calls.

Req-13:

A solution MUST prevent misuse of the emergency infrastructure by unauthorized entities.

Req-14:

Emergency notification systems SHOULD identify the message and

notification originator, preferably in a cryptographically secure manner.

Req-15:

A solution MUST offer sufficient details of the emergency situation.

Req-16:

A solution MUST support integrity protection of early warning notifications.

Req-17:

A solution MUST provide a mechanism for testing authority-to-individuals early warning messages just as test support is provided by individuals-to-authority emergency services.

Req-18:

Devices should be able to recognize alerts that requires that the device override user interface configurations such as vibrate-only mode. (For example, a school closing advisory due to snow may not require such an immediate alert in the middle of the night.)

4. IANA Considerations

This document does not require actions by IANA.

5. Security considerations

This document outlines requirements and security security requirements are a part of them.

6. Acknowledgments

This document reuses requirements captured outside the IETF, namely ETSI (with [ETSI-TS-102-182]), and the 3GPP (with [3GPP-TR-22.968]). We would like to thank the authors of these specifications for their work. Note, however, that only a small subset of the requirements have been reflected that do not relate to specific deployments, user interface aspects, detailed regulatory requirements, management and operational considerations, and non-IP specific technologies.

We would like to thank Leopold Murhammer for his review in July 2007.

7. References

7.1. Normative References

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

7.2. Informative References

[3GPP-TR-22.968]
, ., "3GPP TR 22.968, V1.0.0 (2007-04), 3rd Generation Partnership Project; Technical Specification Group Services and System Aspects; Study for requirements for a Public Warning System (PWS) Service (Release 8)", December 2006.

[ETSI-TS-102-182]
, ., "ETSI TS 102 182, V1.2.1 (2006-12), Technical Specification, Emergency Communications (EMTEL); Requirements for communications from authorities/ organizations to individuals, groups or the general public during emergencies", December 2006.

Authors' Addresses

Steve Norreys
BT Group
1 London Road
Brentwood, Essex CM14 4QP
UK

Phone: +44 1277 32 32 20
Email: steve.norreys@bt.com

Hannes Tschofenig
Nokia Siemens Networks
Linnoitustie 6
Espoo 02600
Finland

Phone: +358 (50) 4871445
Email: Hannes.Tschofenig@gmx.net
URI: http://www.tschofenig.priv.at

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

Full Copyright Statement

Intellectual Property

ietf-ipr@ietf.org.