Mobile Emergency Announcements with Really Simple Syndication (RSS 2.0)

Yrjo Raivio
Telecommunications Software and
Multimedia Laboratory,
Helsinki University of Technology (TKK),
Finland
yrjo.raivio@tkk.fi

Ronja Addams-Moring
Telecommunications Software and
Multimedia Laboratory,
Helsinki University of Technology (TKK),
Finland
ronja.addams-moring@tkk.fi

ABSTRACT

Broadcasting methods, such as the radio, the television and sirens, have been the main choices for delivering emergency announcements (EA) – also called public warnings, emergency alerts or citizens warnings – during the last 60 odd years. Unfortunately, broadcast EAs do not reach all people, and the reason for the EA and the actions required can remain unclear. Today, the high penetration of personal mobile phones offers new options to authorities. As a result, a new research and implementation area, Mobile Emergency Announcement (MEA), has emerged. The GSM Short Message System (SMS) is already deployed for MEA delivery. Simultaneously, in the World Wide Web (WWW) a novel news delivery technology, called Really Simple Syndication 2.0 (RSS) is spreading. This paper describes a concept for how RSS can be harnessed for MEA use. First, MEA requirements are briefly reviewed. Second, the eXtended Markup Language (XML) based Common Alerting Protocol (CAP) and the syndication protocol RSS 2.0 are presented. Third, the central implementation issues are presented. Finally, the proposed solution is critically reviewed.

Keywords

Mobile Emergency Announcement, MEA, Common Alerting Protocol, CAP, Really Simple Syndication, RSS, Public Warning, Citizens Warning.

INTRODUCTION

In an emergency or crisis, the people who are affected by it, look to the authorities for information: they expect timely warnings and instructions about where to go and what to do. Especially in the earlier phases of the emergency management and preparedness lifecycle: planning, mitigation and alerting, the ability to get the necessary information to the affected people fast is crucial for minimizing losses. However, it is quite difficult to predict, which information channels or communication technologies will, during an emergency, reach a large enough percentage of the population. Information and communication technology (ICT) offers so many choices for today's consumers, from China to Chihuahua, that predictably reaching over 50% of any population has become something of an emergency management authority's nightmare.

The answer arising in response to this problem seems to be multi-channel emergency announcement (MCEA) systems (McGinley and Turk, 2004; Zimmermann, 2005; Scherner and Fritsch, 2005). MCEA systems forward the emergency announcements (EA) – also called public warnings, emergency alerts or citizens warnings – to the target population (the intended recipients) through multiple communication channels and thus in multiple formats. However, the choice still has to be made: which ICT solutions will be used for the recipient part of the MCEA system? The authorities value a write-once sender part of a MCEA system, where the content of each EA is entered only once, so that inconsistencies in EA content can be avoided (McGinley et al., 2004; Zhao, Addams-Moring and Kekkonen, 2005). Somewhat contrastingly, the individuals in the target population should get the EAs through their ICT of choice, i.e. the communication devices, services or channels they are most likely to be using at the time of the emergency, regardless of whether it is television, radio, a mobile phone, a pager, an Internet telephoning system (e.g. Skype), WWW, e-mail, voice mail or something else. This places considerable demands on the automatic construction of EAs for different technical formats, but at least on prototype level many of these problems have been solved (McGinley et al., 2004).

An important part of any MCEA system is one or more mobile emergency announcement (MEA) subsystems. As people increasingly often carry at least one personal device with communication capabilities with them, EAs sent directly to their pockets, purses and backpacks can provide a better population reachability than any other MCEA channel. On the other hand, today Internet-connected networks also cover most of the world and thanks to mobile packet data networks, such as the general packet radio service (GPRS) and various third generation mobile networks (3G), even many mobile phones are capable of utilizing Internet data. Therefore, it is natural to study whether combining the mobile and Internet domains could be a solution for MEAs.

Context of This Study

The general context of this study is **the challenge of emergency announcements** (EA). We define this challenge as follows:

> How do authorities get information to the population affected by the emergency in such a manner that, based on the information, as many people as possible act appropriately and thus losses (especially of human life and health) will be minimized;
>
> - in the time-constrained and emotionally charged, uncertainty-heavy and thus often rumor-ridden atmosphere of an emergency;
> - when the affected population and the available ICT both are heterogeneous in various ways;
> - when all information has to be understandable based on everyday human communication habits, which we know to be imprecise and prone to misunderstandings;
> - and when we have to rely on communication technologies that are likely to be directly affected by the emergency or overloaded due to everyone’s heightened need for information, or both.

We believe that EAs and MCEA systems will succeed if they manage to efficiently utilize existing ICT and established ICT use patterns within the target population, without compromising the most essential requirements for EAs and MCEA systems (McGinley et al., 2004; Samarajiva, Anderson and Zainudeen 2005; Zhao et al., 2005).

Scope and Goals of This Study

The aim of this study is to help solve one technical part of the challenge of emergency announcements, as it is defined above. In this paper we analyze one up-and-coming information syndication technology, Really Simple Syndication 2.0 (RSS), for MEA suitability. So far RSS 2.0 has been proposed only to be used for alerting emergency authorities (Baker and Carpenter, 2005). We want to know if there are reasons to include RSS 2.0 as a subsystem in a plan for a multi-channel emergency announcements (MCEA) system. Neither the necessary integration work of RSS 2.0 into the MCEA nor an analysis of the cost structures involved are in our scope.

The general research question that we aim to answer is if a “pull” type technology, such as RSS 2.0, can, with carefully balanced settings, fulfill well enough the “push” technology requirement of MEA systems (Valtonen et al., 2004; Zhao et al., 2005). The specific research question that we aim to answer is if RSS 2.0 can fulfill the authenticity, integrity and non-repudiation requirements for EA, MEA and MCEA systems (FCC, 2004, p. 17; McGinley et al., 2004, p. 5; Valtonen et al., 2004; Scherner and Fritsch, 2005; Zhao et al., 2005).

BACKGROUND

Requirements for Mobile and Multi-Channel EA Systems and existing solutions

Requirements for EA, MEA and MCEA systems have been discussed by at least Held (2001), FCC (2004), McGinley et al. (2004), Valtonen et al. (2004), Samarajiva et al. (2005) and Scherner et al. (2005). A compilation of requirements for MEA systems has been made by Zhao et al. (2005). The four main requirement categories for MEA systems, according to Zhao et al. (2005), are **security:** authenticity, integrity, non-repudiation, etc.; **technical capability:** robustness, throughput, initiative transmission, locating ability, timing, etc.; **operational efficiency:** coverage range, population reachability, cost, prospects of the technology (life cycle length) etc.; and **usability** (“psycho-social reliability” in their terms): payload size, understandability, consistency, etc.

On the whole, cellular networks (today mostly used by mobile phones) fulfill the operational efficiency requirements well. At least in the Netherlands and in Thailand, GSM short messages service (SMS) based MEAs are in official use (Eysink Smeets and Sillem, 2005; IOC, 2005). In Great Britain, a commercial SMS MEA service exists (Easytext.com, 2006). The global interest for GSM Cell Broadcasting Service (CBS) based MEAs is growing, too (O'Brien, 2006).

However, both SMS and CBS based MEAs have limitations. They offer a restricted information space (160 characters) and thus little possibilities for multilingual instructions and no possibilities for visual material (such as evacuation maps). Also, SMS messages are based on a one to one type of information channel, which does not scale well and has privacy concerns (Valtonen, Addams-Moring, Virtanen, Järvinen and Moring, 2004).

How fast a large enough percentage of the target population can receive an EA is an issue that becomes critical for SMS MEAs, because cellular networks have not been designed for broadcasting communication. The new specifications, CBS and multimedia broadcast multicast system (MBMS), do help considerably, but it may take quite some time before cellular networks widely support these as MEA technologies (O'Brien, 2006).

Common Alerting Protocol (CAP)

Contrastingly, the Common Alerting Protocol (CAP) has been designed for one-to-many message delivery. CAP is an open (non-proprietary) digital message format, standardized by the Organization for the Advancement of Structured Information Standards (OASIS). CAP enables flexible and versatile alert management implementations over various transport solutions (e.g. the Internet). CAP defines the alert message formats on top of the XML Schema (the "grammar" of the XML language). The XML Schema provides flexibility for the message structure and new customized fields can easily be added. The key benefit of CAP is the reduced alert message complexity due to standardized XML syntax, which minimizes the need for expensive adaptations. (Jones and Botterell, 2005)

CAP itself does not include any transport mechanism but it can be integrated, for example, into an HTTP based Web Services system. CAP supports some advanced capabilities, including geographic dimensioning, multilingual support, digital encryption and signatures, digital images and audio. Security can be managed with the Web Services Security framework, defined by the World Wide Web Consortium (W3C, 2006). There are ready made tools for message authenticity, integrity and confidentiality. (Jones et al., 2005)

When comparing the CAP specification to the requirements listed above, CAP fulfills well those requirements that can be met on the protocol level. This is no surprise as CAP was created by emergency management experts.

Really Simple Syndication (RSS) and ATOM

However, any XML based document, also a CAP alert, is basically static and does not support dynamic information, which again is produced in abundance in every emergency situation. Thankfully, many news WWW sites (from CNN.com and BBC.co.uk to the.honoluluadvertiser.com) have already solved a similar information update challenge. To make easily changes to news WWW pages visible to regular readers of the pages, a new concept called "channel", "feed" or "syndication" was defined. These feeds are XML incarnations of the HTML news sites. The key novelty of the system is the client side reader software, which converts machine coded XML messages to human understandable text, pictures, voice and video. The reader client periodically polls the news site(s) of interest, and each time the news feed on a server has been updated, the new headline or headlines are uploaded to the reader. This process can be automated so that the reader can independently follow hundreds of news sites on behalf of the user. The user will notice the new article headlines on the PC or mobile phone screen, and can decide which full articles she or he will fetch by clicking the header. Depending on the importance of the news source, the user can define the polling time from minutes to days. Currently, both separate syndication readers and plug-ins for browsers are available. Also aggregators based on WWW pages can be used to follow these feeds.

During the short history of syndication protocols several protocol versions have been developed. The history of WWW syndication started in 1997, and today, two major alternatives are on the table. The most popular syndication protocol is called Really Simple Syndication, version 2.0 or just RSS (Berkman Center, 2005). It had several predecessors, but different RSS versions are not backward compatible, although some RSS readers can support also older formats. There is also another, closely related syndication format, ATOM. In July 2005 the ATOM 1.0 specification was published and it was accepted as an Internet Draft (Nottingham and Sayre, 2005). The technical differences between RSS 2.0 and ATOM are small. Both RSS and ATOM can encapsulate CAP inside the feed. Most RSS readers support ATOM format, too. Figure 1 describes a protocol stack supporting the CAP protocol. In the figure the two syndication protocols (RSS and ATOM) are presented as alternatives to each other.

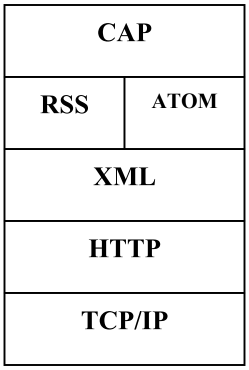


Figure 1. Emergency Announcement protocol stack

Relating to EAs the only considerable difference between RSS and ATOM concerns security. Both RSS and ATOM can apply Web Security encryption and signature technologies to bulk bits of data, but ATOM can also use them for separate feeds. Until now RSS reader and aggregator implementers have been reluctant to add optional security features to their readers, as RSS has been based on a "news only" concept – plain text, free content, rapid creation and easy consumption – and security requirements have had low priority. However, the wider deployment of RSS technology, and the emerging commercial information aggregation and distribution feeds, create more pressure towards security functions. For example, Microsoft (2006) has announced the integration of a RSS reader into its next operating system, and for mobile phones several commercial RSS readers are available already today.

THE PROPOSED IMPLEMENTATION

Design principles

Based on that RSS 2.0 is more widely deployed than ATOM (the future success of ATOM is still unclear), we continue this evaluation with RSS 2.0. RSS 2.0 could be used for MEAs also without CAP, but encapsulating CAP inside a RSS feed gives advantages. Most importantly, CAP contains the necessary emergency extensions, flexibility and security features, and with standardized CAP, costly adaptations can be minimized.

Then how do we get the RSS-CAP MEA feeds to mobile phones and other widely used personal communication devices? Packet data compatible mobile devices can utilize any mobile packet data network. RSS feed technology already works well with second generation cellular networks (GSM/GPRS), and 3G and Wireless Local Area Network (WLAN) accesses provide more bandwidth and also better locating accuracy.

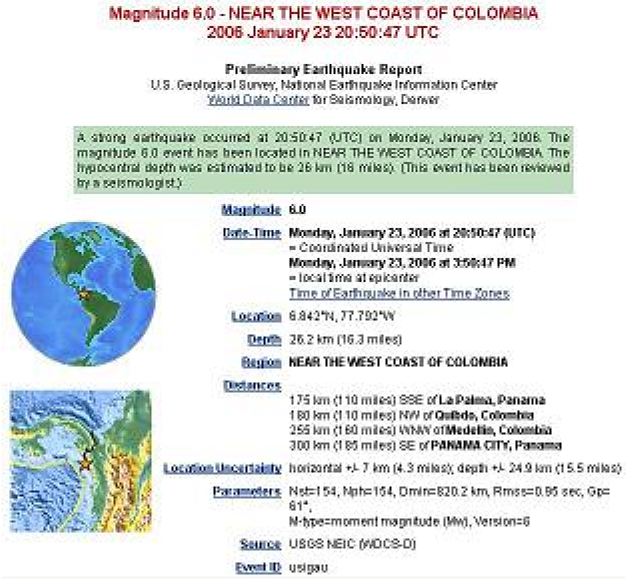
MEA handling on the end user device requires that a specific MEA application, on top of or integrated into the RSS reader, must be developed. Otherwise the MEA can be accidentally ignored. MEA handling can use filtering based on the location, severity and urgency indicated in the MEA. The RSS-CAP MEA feed can include a full list of MEAs, but with filtering, the end user device will detect only the MEAs that match the filtering criteria.

If needed, geographic information can be added to a RSS-CAP MEA feed, such as maps of the disaster area and evacuation routes. Governments may want to control the end user MEA applications and determine their required functionality in a similar way as the functionalities concerning the general emergency number 911 (for the U.S.) or 112 (for the EU) are defined today. A specific MEA application could also support additional security features such as signatures and encryption, as described later. A more critical issue, however, from the mobile networks' point of view, is the needed network capacity and the scalability of a RSS-CAP MEA feed, which are addressed next.

Scalability issues

A RSS-CAP based MEA system load would normally be close to constant because clients poll the server with periodic requests, which are distributed randomly and evenly enough. If the server has no new updates, the HTTP connection can be immediately terminated utilizing HTTP Conditional Request Headers (Dixit and Wu, 2004). The server will notify the client through the HTTP layer that there is nothing new to be downloaded. If the server has new updates, the new MEA headlines are downloaded to the client, and it will evaluate, based on the location data and other preconfigured rules, if the full MEA should be fetched and if the user should be alerted.

The polling time should be reasonably short to achieve an almost real time service, but simultaneously the network load should not exceed the network's capacity. If the chosen polling time was 5 minutes, it would mean that clients will receive the MEA with a delay that is evenly distributed between 0 and 5 minutes, with an average delay of 2.5 minutes. A RSS 2.0 test site by the U.S. Geological Survey (USGS) has examples of emergency related RSS-CAP feeds (USGS, 2006). Each RSS poll request consumes just a few hundreds of bytes of data, while a typical aggregation page including the headlines has the approximate size of 2 kB. This includes also a link to the relevant HTML page, which can have maps and other visual data, and which is downloaded only upon the user's request and only once. Figure 2 shows such a page. In this USGC example, such HTML pages have an average size of 20 kB.



Magnitude 6.0 - NEAR THE WEST COAST OF COLOMBIA
2006 January 23 20:50:47 UTC

Preliminary Earthquake Report
U.S. Geological Survey, National Earthquake Information Center
World Data Center for Seismology, Denver

A strong earthquake occurred at 20:50:47 (UTC) on Monday, January 23, 2006. The magnitude 6.0 event has been located in NEAR THE WEST COAST OF COLOMBIA. The hypocentral depth was estimated to be 26 km (16 miles). (This event has been reviewed by a seismologist.)

Magnitude 6.0

Date-Time Monday, January 23, 2006 at 20:50:47 (UTC)
= Coordinated Universal Time
Monday, January 23, 2006 at 3:50:47 PM
= local time at epicenter
Time of Earthquake in other Time Zones

Location 6.842°N, 77.792°W

Depth 26.2 km (16.3 miles)

Region NEAR THE WEST COAST OF COLOMBIA

Distances
175 km (110 miles) SSE of La Palma, Panama
180 km (110 miles) NW of Quibdo, Colombia
255 km (160 miles) WNW of Medellin, Colombia
300 km (185 miles) SE of PANAMA CITY, Panama

Location Uncertainty horizontal +/- 7 km (4.3 miles); depth +/- 24.9 km (15.5 miles)

Parameters Nst=154, Nph=164, Dmin=820.2 km, Rmss=0.86 sec, Gp= 61°,
M-type=moment magnitude (Mw), Version=6

Source USGS NEIC (WDCS-D)

Event ID usigau

Figure 2. Emergency Announcement in HTML format (U.S. Geological Survey, 2006)

If we can assume that new EA content is created judiciously also during a full blown crisis, then we can estimate what the end user device and server (network) loads could be, for the USGS example above. For an end user device the total load can be some 100 to 200 kB per day, depending on the MEA feed update frequency and the number of downloads of HTML pages. The polling frequency does not essentially impact the end user device's load due to HTTP Conditional Request Headers, but server capacity must be more closely analyzed. The most critical value is a server's maximum response rate to the HTTP requests. For example, 1 million clients with a 5 minute polling time and an even distribution of polling activities will create 3333 hits per second to the server. If each hit initiates a fetch of the alarm aggregation page (2 kB), the server's peak output capacity requirement can reach 52 Mbit/s. In the worst case each client will also download the HTML page (20 kB), so the required server peak output capacity can be up to 570 Mbit/s, so load distribution with server clustering should effectively solve the scaling issues.

Security and privacy issues

In pull technologies based MEA solutions, such as RSS-CAP MEA feeds, where the end user devices automatically poll the MEA feed, the security requirements are slightly different from those for push technologies, where the MEA forwarder part forces the MEAs into the end user devices. With both push and pull methods, however, we must first guarantee that the relevant emergency centers have also the *technical* authorization to distribute EAs.

One serious security threat with the push method is EA fraud (e.g. organized crime could profit from reactions to fraudulent EAs), and that is why it is necessary to confirm the authenticity of each pushed EA. In the pull type approach the server side and EA authentication are less critical, if we can guarantee that (M)EA clients subscribe only to authorized (M)EA feeds. This server side authentication can be provided with the W3C Signature and Key Management specifications (W3C, 2006). RSS-CAP MEA feeds can be signed by the EA authority's signature and end user devices can verify the used public keys from the underlying Public Key Infrastructure (PKI) system, which naturally must exist. The signature thus also offers the integrity protection and non-repudiation features, i.e. the sender of a RSS-CAP MEA can be checked and held accountable afterwards.

Normally, MEAs should be available for free to anybody, and in this case users do not need to be authenticated or authorized. However, for commercialized MEA services, a RSS-CAP MEA system should offer a possibility for user authentication, too. If it is needed, the user side authentication can be solved with HTTP Basic and Digest Access Authentication methods, which are used by many WWW sites today.

Especially the pull method, where pre-identifiable servers are open for requests, is vulnerable to Denial-of-Service (DoS) attacks, which are in practice impossible to prevent. With a clustered and decentralized server architecture the risk for a fully successful DoS attack can be minimized. Also, the multi-channel EA system that the RSS-CAP MEA system would be a part of, per definition offers other (M)EA channels if one is temporarily unavailable.

Message encryption can be required to guarantee confidentiality. In a RSS-CAP MEA system, encryption can be unnecessary because MEAs are generally public information. However, if the system is used also to distribute confidential information, or if the timing of the MEA is crucial (e.g. a bridge must be fortified before an evacuation route can safely be announced), the MEA contents should be encrypted. The XML specification set (W3C, 2006) includes an encryption standard. Encryption can be implemented also on the transport layer using Secure Socket Layer (SSL), Transport Layer Security (TLS) and certificates. An XML based solution is a natural choice if the signature and key management parts already exist. If they do not, the system scalability can become a problem.

Virus risks with RSS are similar to any WWW browsing. RSS readers normally store the content to the memory of the end user device and virus scanners can be used to detect malicious code. However, if users subscribe only to trusted sites, the risk for viruses should be small. The most secure way could be that authorities for each country or region provide a portal for the trusted MEA feeds and maybe also include links to similar sites in other areas.

The main security advantage of pull technologies based MEA solutions is better privacy, because the update method decentralizes the locating functionality and MEA selection logic to the end user devices. Thus neither authorities nor MEA or MCEA administrators need to keep records of the phone numbers or the location data of the clients.

Locating end user devices

We assume that a RSS-CAP MEA feed will only cover MEAs for a certain geographical area, and when the area changes, a new MEA feed must be found. Depending on the MEA types distributed, the geographical area can vary from one city to a whole country or region. A mobile end user device should support an automatic reconfiguration procedure that updates the new MEA feeds into the device's memory during a handover or roaming situation, for example when traveling abroad. One solution is to pre-configure (some) MEA feeds into the MEA application.

For RSS-CAP MEAs it would be beneficial if an end user device always knew its geographical location, at least with some accuracy. For most emergency cases the accuracy of current mobile locating technologies is already good enough. However, the usability of the MEA system improves with real time location data. At the moment this is not the case for mobile phones, but, for example, a GSM phone has to explicitly ask its location from the Gateway Mobile Location Center (GMLC) network element. Currently location services also cost a lot, but for emergency purposes location information should be free, just as location tracing for the 112 or 911 emergency calls is. Because the CAP protocol includes incident co-ordinates and watch out area details, a MEA application could compare the end user device's actual location to the disaster co-ordinates, and draw conclusions on if the MEA requires prompt attention. As a minimum, the RSS-CAP MEA system should automatically detect if the mobile phone moves to a new location. This feature requires that the end user MEA application has access to location data.

Because of the approximative nature of current mobile phone location data, the RSS-CAP MEA approach would suit best such MEAs that need to reach a large group of people in scattered, geographically approximative areas, and not so well if we need to warn a single individual or a few persons in a very specific location. An incident similar to the Indian Ocean Tsunami in 2004 could be a use case where a RSS-CAP MEA system would be very useful.

DISCUSSION

Advantages of the RSS-CAP MEA concept

A RSS-CAP MEA is especially useful, if we need to reach tourists, who are traveling abroad and located in scattered areas. In addition to SMS MEAs, a RSS-CAP MEA feed is one of the few currently promising options for authorities to reach their own nationals in an emergency abroad. In such a scenario the SMS MEA channel and RSS-CAP MEA feeds could support each other for better target population coverage. The greatest advantage of RSS is the possibility to tailor MEAs flexibly to emergency or information announcements: RSS and CAP are suitable for short and simple messages, but also a large group of extensions are supported. Location data and maps could easily be added to the information and they could help people to better recognize the severity and the likely impact of the emergency. In recent disasters, such as the Indian Ocean Tsunami, the lack of information was one of the major problems for those who survived and also for their relatives. RSS-CAP MEA feeds could supply both with reliable information fast.

Additionally, a RSS-CAP MEA solution should scale well to large numbers of users, because the system load is evenly enough distributed and remains mostly constant (naturally depending on how often new EA content is created). A pull type technology can be used also for high priority MEAs if a short enough polling time is set. A push method maybe should be applied only to highest priority MEAs because otherwise MEAs can lose their effectiveness (become "spam"). In contrast to SMS MEAs, RSS-CAP MEAs offer better privacy, as no centralized registers of users or tracing of end user devices are required. Last but not least, RSS 2.0 will likely be included as a standard part in new versions of major operating systems for both personal computers and mobile phones.

Disadvantages of the RSS-CAP MEA concept

RSS-CAP MEA has also disadvantages. At the moment RSS penetration is still low (Grossnickle, Board, Pickens and Bellmont, 2005). The technical requirements for RSS-CAP MEAs are demanding, and an advanced network and end user device support is needed. It is possible that the RSS system is suitable only for developed countries or backing up main EA channels, such as sirens and radio. The major technical challenge concerns how to get the correct MEAs to the mobile device's screen, i.e. MEAs should offer *just on time* service with accurate information for the correct target group. Therefore location data is needed, and mobile phones today do not automatically have it. Restrictions typical for mobile devices, such as display size and battery life time, also set limits. The polling solution will create extra charges that can be considerable in some countries. The RSS-CAP MEA system availability can also become a problem in case of inexpert server side dimensioning or DoS attacks.

CONCLUSIONS

We have analyzed the literature on an information syndication technology, Really Simple Syndication 2.0 (RSS), to establish if it would be suitable for mobile emergency announcements (MEA) and thus, if there would be reasons to include RSS 2.0 as a subsystem in a plan for a multi-channel emergency announcements (MCEA) system. We found that even though RSS 2.0 is a "pull" type of technology, which demands that the end user devices actively and regularly enough poll the MCEA forwarder part, RSS 2.0 can fulfill well enough the "push" technology requirement of MEA systems, by utilizing the Conditional Request Header of HTTP and optimized polling frequencies. We also found that RSS 2.0 can fulfill the authenticity, integrity and non-repudiation requirements for EA, MEA and MCEA systems and that Common Alerting Protocol (CAP) messages can be encapsulated inside RSS.

Furthermore, RSS 2.0 is most likely being included as a standard part in the newest versions of major operating systems for both personal computers and mobile phones, and the RSS-CAP based MEA concept offers clear advantages concerning user privacy. Therefore, we recommend that feasible cost structures for pull-type technology based MEA feeds be studied next and that future MCEAs, at least in developed countries, be planned for easy inclusion of RSS-CAP as one of the MEA delivery channels.

CONTRIBUTION REPORT AND ACKNOWLEDGMENTS

Considering that in the future this paper may be used as a part of a thesis, we volunteer this information.
Guarantor: Yrjo Raivio (YR). **Scientific contribution and participation in the writing**: Ronja Addams-Moring (RAM) suggested that students evaluate different ICTs for MEA and MCEA suitability. YR suggested that he evaluates RSS 2.0. RAM tutored YR when he did the literature analysis for and wrote the first full-length draft of this paper. YR selected the issues to be addressed and did the analysis of all the addressed XML based data formats mostly independently. RAM's primary responsibility was aligning the work with emergency management realities, especially with MEA and MCEA requirements. Based on discussions with YR, RAM edited the whole paper before submission. After the reviews, both YR and RAM edited the paper based on reviewer comments.
Accepting of text: Both authors have accepted the text of this final paper via e-mail on March 15, 2006.

Acknowledgements: We thank Göran Schultz and Jaakko Rajaniemi for their comments on the first draft.

REFERENCES

1. Baker, F. and Carpenter, B. (2005) Structure of an International Emergency Alert System. At: *http://ietf.mirror.netmonic.com/draft-baker-alert-system-00.txt*. Referenced: 15 Mar 2006.
2. Berkman Center for Internet & Society at Harvard Law School (2005) RSS 2.0 Specification. At: *http://blogs.law.harvard.edu/tech/rss*. Referenced: 15 Mar 2006.
3. Dixit, S. and Wu, T. (2004) Content Networking in the Mobile Internet, p. 57. John Wiley & Sons, Inc.
4. Eazytext.com (2006) C.A.T.S. City Alert Texting System. At: *http://www.cityalert.co.uk/static/index.htm*. Referenced: 15 Mar 2006.
5. Eysink Smeets, M.W.B. and Sillem, S. (2005), Intelligent SMS as an effective public warning system: the inspiring results of a Dutch pilot project, In B. Carle and B. Van de Walle, editors, *Proceedings of the 2nd International ISCRAM conference.* Tilburg University. Available at http://www.iscram.org.
6. FCC, Federal Communications Commission, USA (2004) Review of the Emergency Alert System. At: *http://www.fcc.gov/eb/Orders/2004/FCC-04-189A1.html*. Referenced: 15 Mar 2006.
7. Grossnickle, J., Board, T., Pickens, B. and Bellmont, M. (2005) RSS - Crossing into the Mainstream, White Paper, Yahoo. At: *http://publisher.yahoo.com/rss/RSS_whitePaper1004.pdf*. Referenced: 15 Mar 2006.
8. Held, V. (2001) Technological options for an early alert of the population. At: *http://www.bbk.bund.de/cln_027/nn_523744/Schutzkommission/SharedDocs/Publikationen/Band_2045.html*. Referenced: 15 Mar 2006.
9. IOC (2005) Towards the Establishment of a Tsunami Warning and Mitigation System for the Indian Ocean. At: *http://ioc3.unesco.org/indotsunami/IOC23/ioc23.htm*. Referenced: 15 Mar 2006.
10. Jones, E. and Botterell, A. (2005) Common Alerting Protocol 1.1, OASIS. At: *http://www.oasis-open.org/committees/download.php/14759/emergency-CAPv1.1.pdf*. Referenced: 15 Mar 2006.
11. McGinley, M. and Turk, A. (2004) Newsbug. Multi-channel public emergency messaging system. Final report. At: *http://www.itri.tv/newsbug/*. Referenced: 15 Mar 2006.
12. Microsoft (2006) Windows Vista Advances for Developers. At: *http://msdn.microsoft.com/windowsvista/about/*. Referenced: 15 Mar 2006.
13. Nottingham, M. and Sayre R. (2005) The Atom Syndication Format. At: *http://www.atomenabled.org/developers/syndication/atom-format-spec.php*. Referenced: 15 Mar 2006.
14. O'Brien, K.J. (2006) Mobile providers resisting SOS alerts. *http://www.iht.com/articles/2006/01/10/business/warnings.php/*. Referenced: 15 Mar 2006
15. Samarajiva, R., Anderson, P. S. and Zainudeen, A. (2005) Interim Concept Paper: Specifications of a National All-Hazards Warning System for Sri Lanka. At: *http://www.lirneasia.net/wp-content/Concept%20Paper%203Feb05_01.pdf*. Referenced: 15 Mar 2006.
16. Scherner, T. and Fritsch, L. (2005) Notifying civilians in time – disaster warning systems based on a multilaterally secure, economic and mobile infrastructure. *Proceedings of the Eleventh Americas Conference on Information Systems*. Omaha, NE, USA.
17. U.S.Geological Survey (2006) RSS/XML and CAP Feeds. At: *http://www.usgs.gov/homepage/rss_feeds.asp*. Referenced: 15 Mar 2006.
18. Valtonen, E., Addams-Moring, R., Virtanen, T., Järvinen, A. and Moring, M. (2004) Emergency announcements to mobile user devices in geographically defined areas. In B. Carle and B. Van de Walle, editors, *Proceedings of the 2004 ISCRAM workshop.* Tilburg University. Available at *http://www.iscram.org*.
19. W3C (2006) W3C Technical Reports and Publications. At: *http://www.w3.org/TR/*. Referenced: 15 Mar 2006.
20. Zhao, S., Addams-Moring, R. and Kekkonen, M. (2005) Building mobile emergency announcement systems in 3G networks. In *Proceedings of Communications and Computer Networks, 2005*. ACTA Press, Calgary, AB, Canada.
21. Zimmermann, H. (2005) Recent developments in emergency telecommunications. In B. Carle and B. Van de Walle, editors, *Proceedings of the 2nd International ISCRAM conference.* Tilburg University. Available at *http://www.iscram.org*.